FORTINET

FortiOS™ Handbook - Security Profiles

VERSION 6.0.3

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

November 15, 2018

FortiOS™ Handbook - Security Profiles

01-603-481091-20181115

TABLE OF CONTENTS

Change log

Date	Change description
October 4, 2018	FortiOS 6.0.3 document release. Minor changes.
July 26, 2018	FortiOS 6.0.2 document release. See "What's new in FortiOS 6.0.1" on page 15
June 5, 2018	FortiOS 6.0.1 document release. See "What's new in FortiOS 6.0.1" on page 15.
March 29, 2018	FortiOS 6.0 document release. See "What's new in FortiOS 6.0" on page 15.

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

The following chapter describes the Security Profile features available on your FortiGate unit, including antivirus, intrusion prevention system (IPS), web filtering, email filtering, data leak prevention, (DLP) and application control. The guide includes step-by-step instructions showing how to configure each feature. Example scenarios are included, with suggested configurations.

Examples include scenarios using web filtering to protect users from inappropriate content, using IPS to protect web servers from attack, and using antivirus scanning to protect your network against viruses and malicious file attachments.

Before you begin

Before you begin using this guide, take a moment to note the following:

Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

Firewall policies limit access, and, while this and other similar features are a vital part of securing your network, they are not covered in this guide.

If your FortiGate unit supports SSL acceleration, it also supports SSL content scanning and inspection for HTTPS, IMAPS, POP3S, and SMTPS traffic.

How this chapter is organized

This FortiOS Handbook chapter contains the following sections:

- What's New in FortiOS 6.0 describes the new security profile features in FortiOS 6.0
- Inside FortiOS highlights the features and benefits of key FortiOS 6.0 components. The technical documentation team maintains these documents as part of the Handbook and as standalone documents which are available at Fortinet's Online Help. Inside FortiOS covers the following security profiles topics:
  - AntiVirus
  - Application Control
  - Intrusion Prevention System
  - Web Filtering
- Security profiles overview describes Security Profiles components and their relation to firewall policies, as well as SSL content scanning and inspection.
- Inspection Modes discusses the FortiGate's inspection modes and how the security profiles function depending on inspection mode.
- AntiVirus explains how the FortiGate unit scans files for viruses and describes how to configure the antivirus options.

- Web filter describes basic web filtering concepts, FortiGuard Web Filtering, the order in which the FortiGate unit performs web filtering, and configuration.
- DNS filter explains how to configure the Domain Name System (DNS) Filter security profile independent of the Web Filter security profile.
- Application control describes how your FortiGate unit can detect and take action against network traffic based on the application generating the traffic.
- Intrusion prevention explains basic Intrusion Protection System (IPS) concepts and how to configure IPS options; includes guidance and a detailed table for creating custom signatures as well as several examples.
- Anti-spam filter explains how the FortiGate unit filters email, how to configure the filtering options, and which actions to take when spam is detected.
- Data leak prevention describes the DLP features that allow you to prevent sensitive data from leaving your network and explains how to configure the DLP rules, compound rules, and sensors.
- ICAP support describes how to offload traffic to a separate server specifically set up for the specialized processing of the traffic.
- FortiClient Compliance Profiles addresses the FortiClient Profiles endpoint protection features and configuration.
- SSL/SSH Inspection presents SSl and SSH content scanning and inspection with your FortiGate.
- Custom Application & IPS Signatures describes how to create custom Application Control and IPS signatures.
- Other security profiles considerations addresses topics like Security Profiles VDOMs, conserve mode, using wildcards and Perl regular expressions, adding External Security Devices, CPU allocation and tuning commands to survive reboot and so on.

What's new in FortiOS 6.0.1

The following list contains new Security Profile features added in FortiOS 6.0.1. Click on a link to navigate to that section for further information.

- "Option for "Suspicious Files Only" for FortiSandbox submissions" on page 62

What's new in FortiOS 6.0

The following list contains new Security Profile features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- "Content Disarm and Reconstruction (CDR)" on page 67
- "FortiGuard virus outbreak prevention" on page 69
- "Overriding the AV engine file scan timeout" on page 70
- "Web filtering local and remote category status" on page 95
- "Threat Feed Connectors" on page 99
- "YouTube Channel Filtering" on page 103
- "Configure IPS options" on page 142 (for more information, see the FortiOS 6.0 CLI Reference)
- "Configuring endpoint protection" on page 187
- "Endpoint compliance checking" on page 189
- "Enforcing FortiClient EMS requirements" on page 190

- "Configuring the FortiClient offline grace period" on page 192
- "SSH MITM deep inspection" on page 207
- "Global security profiles across Virtual domains (VDOMs)" on page 230
- "Control how sessions are distributed to Fortinet processes" on page 235
- "Excluding industrial IP signatures" on page 236
- Extended UTM logging (for more information, see the FortiOS 6.0 CLI Reference)

Inside FortiOS: AntiVirus

AntiVirus uses a suite of integrated security technologies to provide against a variety of threats, including both known and unknown malicious codes (Malware), plus Advanced Targeted Attacks (ATA), also known as Advanced Persistent Threats (APT).

Advanced protection against malware and APTs

Malware and Advanced Persistent Threats can cause significant damages to today's organizations. These malicious codes are commonly designed to steal valuable data, gain unauthorized access, or cause products to degrade. FortiOS's AntiVirus is an industry-proven anti-malware security solution with robust features and deployment options

FortiOS offers the unique ability to implement both Flow- and Proxy-based AV concurrently, depending on traffic type, users, and locations. Flow-based AV offers higher throughput performance while proxy-based solutions are useful in mitigating stealthy malicious codes. The AV detection capabilities are further enhanced with complementary security features and external sandbox integration.

By utilizing the unique Content Pattern Recognition Language (CPRL) built into the FortiASIC Content Processor, FortiOS is able to deliver high performance and low latency anti-malware capabilities. This real-time protection is backed by a team of worldwide researchers.

Highlights

- Certification from multiple industries for best-in-class security and capacity with proven coverage and high performance.
- Multi-layered protection with extended AV components and external file analysis integration.
- Comprehensive remediation actions such as file quarantine and knowledge tools.

Key Features & Benefits

Robust feature set	Allows the flexibility to deploy appropriate protection according to security needs and infrastructure designs.
High performance utilizing FortiASIC and patented CPRL AV signatures	Low latency and high capacity ensures that business applications are not affected while security is enforced.
Backed by FortiGuard Labs that deliver real-time protection	Critical digital assets are covered by continuous protection against latest threats.

Features

Industry's validated protection

FortiOS anti-malware components and FortiGuard AV signatures periodically undergo numerous authoritative certifications. These independent certifications demonstrate that the solution offered is of the highest standard in performance and accuracy, ensuring organizations are truly protected.

Fortinet has been consistently ranked among the top vendors for Virus Bulletin's RAP (Reactive And Proactive) bimonthly tests. This test measures a product's detection rates over the freshest samples available, as well as samples not seen until after product databases are frozen, thus reflecting both the vendor's ability to handle the huge quantity of newly emerging malware and accurately detect previously unknown malware.

Real time protection

The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content-level threats via the experienced FortiGuard global network is backed by over 200 researchers. With the release of FortiOS 5.6, botnet protection is part of the FortiGuard AntiVirus contract.

FortiGuard AV service quick facts

- 95,000 malware programs neutralized per minute
- 1.8 Million new and updated AV definitions per week
- Hourly updates of the AV signature database
- 190 TB of threat samples till date

Organizations can also engage the FortiGuard Premier Signature Service, which provides enhanced virus detection and threat analysis support. This service offers submissions for custom AntiVirus signatures on a daily basis, offering prioritized support with guaranteed response times. With the release of FortiOS 5.6, botnet protection is part of the FortiGuard AntiVirus contract.

Unique proxy- and flow-based AV

FortiOS offers organizations the flexibility to select the most appropriate inspection method for different network sessions. This can be implemented by defining policies that match specific source objects (IP, IP ranges, users, and devices), destination objects, applications, and schedules with different AV profiles.

Flow-based AV relies on IPS technology where packets are inspected in real-time and matched against the AV signature database. It offers lower latency and higher throughput than Proxy-based AV. Flow-based AV is recommended for inspecting traffic that requires spontaneous user experience or when serving as an additional AV protection layer.

FortiOS's Proxy-based AV offers the most secure AV protection as it's able to inspect more protocols and provides replacement messages on wider range of applications.

AV acceleration with Content Processor

The FortiASICS Content Processor (CP) accelerates content processing traditionally performed completely by the CPU. The CP reduces the resources required by the CPU when matching an incoming file against the signature database, thus improving system performance and stability.

Proactive protection using patented CPRL

Compact Pattern Recognition Language (CPRL) is a patented and proprietary programming language that allows for further inspection of common patterns to not only protect against threats and their variants but also to predict tomorrow's zero-day malware. It allows FortiGuard analysts to describe entire families of malware with a single program, instead of the traditional signature- based "one signature, one variant" model used by other vendors. With fewer signatures to match, throughput performance and latency naturally improve.

Intelligent behavioral evaluation

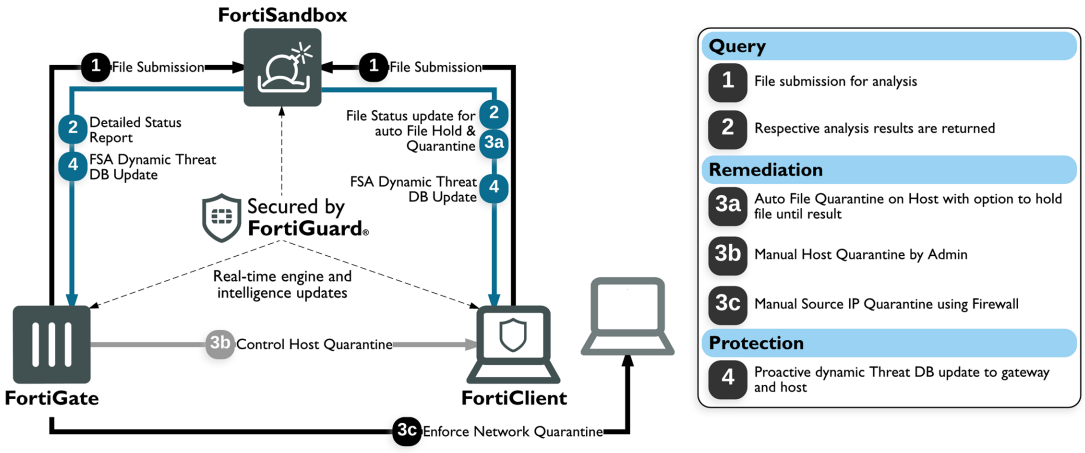
Signature-based security alone is no longer sufficient; it is now critical to understand how devices on your network are behaving. Threat Weight scoring provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real-time.

This unique system attaches predefined scores to various malicious network activities discovered by IPS, application control, URL filtering, etc., to determine the top suspicious users. Administrator can then further inspect these users to undercover unknown threats or APTs via FortiView.

External file analysis integration

FortiOS offers organizations the ability to adopt robust ATP (Advanced Threat Protection) framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files. To detect unknown threats, zero-day, and targeted attacks, the FortiGate can engage external resources to perform additional file analysis. Files can be submitted to an on- premise appliance (FortiSandbox) or cloud-based service (FortiSandbox Cloud) after both proxy-based and flow- based AV processing.

It is also possible to configure the FortiGate to automatically receive dynamic signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list. In addition, if the organization deploys integrated endpoint control with FortiClient, an administrator can instruct an infected terminal to self-quarantine.



File filtering

File filtering using data leak prevention (DLP) on the FortiGate offers an effective ways to stop unwanted file transmission instantly. Administrators may implement granular file controls by defining protection profiles using filenames or nearly 50 different file types over mail, web, and file download protocols.

File quarantine

FortiOS offers sophisticated file quarantine capabilities that allow organizations to archive suspicious or blocked files for further examination or to release false positives.

Anti-bot

Organizations may prevent, uncover, and block botnet activities using FortiOS Anti-Bot traffic pattern detection and domain and IP reputation services supplied in real-time by FortiGuard threat experts.

User notification

User notifications are helpful in reducing administration and support burdens, as well as providing user education. FortiOS is able to automatically replace blocked attachments and downloads with detailed information sent to E-mail, FTP, or web users.

Monitoring, logging, and reporting

FortiOS empowers organizations to implement security best practices that require continuous examination of their threat status and adaptation to new requirements. The FortiView widgets provide useful analysis data with detailed and contextual session information, which can be filtered, ranked, and further inspected. System events can also be archived via logs, which in turn can generate useful trending and overview reports.

FortiOS also offers robust in-built E-mail and SMS alert systems, as well as integration with external threat management systems using SNMP and standard-based Syslogs.

Inside FortiOS: Application Control

Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols.

Enhance control and network visibility

Controlling and monitoring applications on a network can seem like a daunting task due to the wide range of available applications. It is no longer an option to simply block or allow TCP and/or UDP ports since most applications do not map to individual ports. For example, controlling traffic on an HTTP or HTTPS port is futile against complex social networking sites and cloud applications.

FortiOS leverages its massive application database to identify applications and their activities while still providing a suitable and sufficient user experience, thanks to FortiASIC Content Processors (CPs), which boost CPU performance. Organizations can adopt more granular control, such as allowing logins but not chatting over selected sites. Traffic shaping may also be applied to the application traffic that is allowed. After applying control measures, continuous monitoring ensures that the measures are effective and allow for changes in application traffic patterns to be managed.

Highlights

- Superior performance using the unique FortiASIC Content Processor that offloads heavy computation from the CPU.
- Flexible implementation with robust deployment modes and granular controls.
- Excellent visibility and management tools that help administrators improve security.
- Application control is a standard part of any FortiCare support contract and the database for Application Control signatures is separate from the IPS database. Access to the database no longer requires a FortiGuard IPS subscription.

Updates for the Application Control signature database requer a valid FortiCare support contract.

- Supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).
- Ability to configure application control by adding individual applications or application categories to security policies when operating in flow-based inspection and NGFW policy-based mode.

Key features & benefits

Identifies and controls application traffic	Allows organization to strengthen security policies by controlling evasive application communications.

Leverages FortiGate's hardware acceleration and software optimization	Offers more security without compromising performance.
Granular control and integration with other FortiOS capabilities	Provides administrators the ability to implement the most appropriate configuration for any given organization.

Features

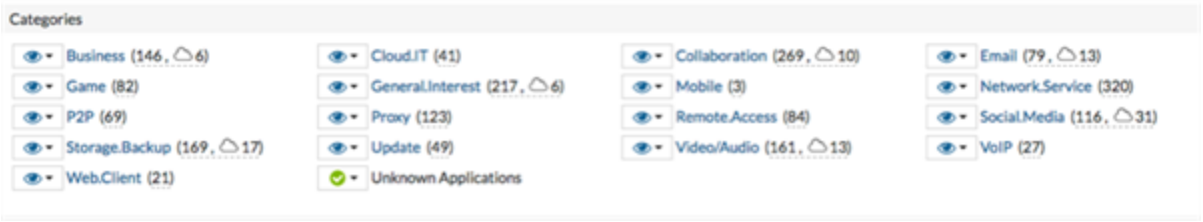
NSS Labs "Recommend" rating for Next Generation Firewall

Fortinet's entry into the NSS Labs Next Generation Firewall Group Test in 2013, 2014 and 2016 received the "Recommend" rating, placing it as one of the top performing systems. NSS Labs uses respectable real-world testing methodologies to measure Next Generation Firewall protection and performance, including application control.

Superior performance with unique hardware architecture

Unlike a traditional security gateway, which relies heavily on CPUs for packet inspection, the FortiGate's unique hardware architecture allows FortiOS to automatically utilize appropriate hardware components to achieve optimal performance. This prevents the CPU from becoming a bottleneck as it performs various functions concurrently.

In support of application control, the Content Processor (CP) is a specialized ASIC chip that handles demanding cryptographic computation for SSL inspection and intensive signature matching. By offloading these processes from the CPU, the FortiGate is able to minimize performance degradation when administrators opt for greater security.



Robust deployment modes

FortiOS supports a wide array of network protocols and operating modes, allowing administrators to deploy the most appropriate security for their unique IT infrastructure. FortiOS also supports a variety of routing and switching protocols.

The FortiGate is able to operate in inline route and transparent mode. It can also operate in offline sniffer mode for passive monitoring of user activities. These different operating modes run concurrently by using virtual systems.

Protection at the edge

With today's BYOD and mobile workforce environment, it is no longer wise to deploy control just at the Internet gateway. Through Fortinet Security Fabric, FortiOS unique wireless and switch controller feature allows organizations to implement better visibility and protection closer to internal devices. Moreover, with FortiClient, administrators can also apply similar policies when mobile users are outside of the protected networks.

Advanced application detection and control

By relying on the FortiOS 3rd Generation IPS engine, the FortiGate is able to inspect many of today's encrypted and evasive traffic, as well as traffic running on new technologies, such as SPDY protocol. The inspection can be applied to both network and IPsec/SSL VPN traffic.

An application and its specific activity are identified using FortiGuard's Application Control database of over 2,500 distinct signatures. These signatures are crafted by researchers across the globe to include applications that may be unique to platforms, regions, and/or languages. It also offers specific application activity identification, such as a Facebook posting or Dropbox file sync. The database is kept up to date via scheduled or manual downloads.

The application database is classified into 20 intuitive categories for ease of use. Administrators may also create specific application overrides that differ from the category settings. These specific applications can be filtered and selected by type of behavior, risk levels, technology type, application vendor and popularity.

Administrators may also apply advanced controls, such as setting up session TTLs for specific applications using CLI commands.

Traffic shaping

Organizations may better utilize bandwidth and protect critical applications by enforcing granular application usage with traffic shaping. Administrators can create various traffic shaping profiles by defining traffic priority and maximum or guaranteed bandwidth. These profiles can then be assigned to targeted applications.

User notification

User education is central to an effective security implementation. In response to this, FortiOS lets you provide user notification when blocking an unauthorized application. The notification appears as an HTML block page for web-based applications.

Advanced notification is possible by implementing Fortinet's browser-embedded frame. And when "off-net" users are denied access, notifications appear via FortiClient's notification pop-ups.

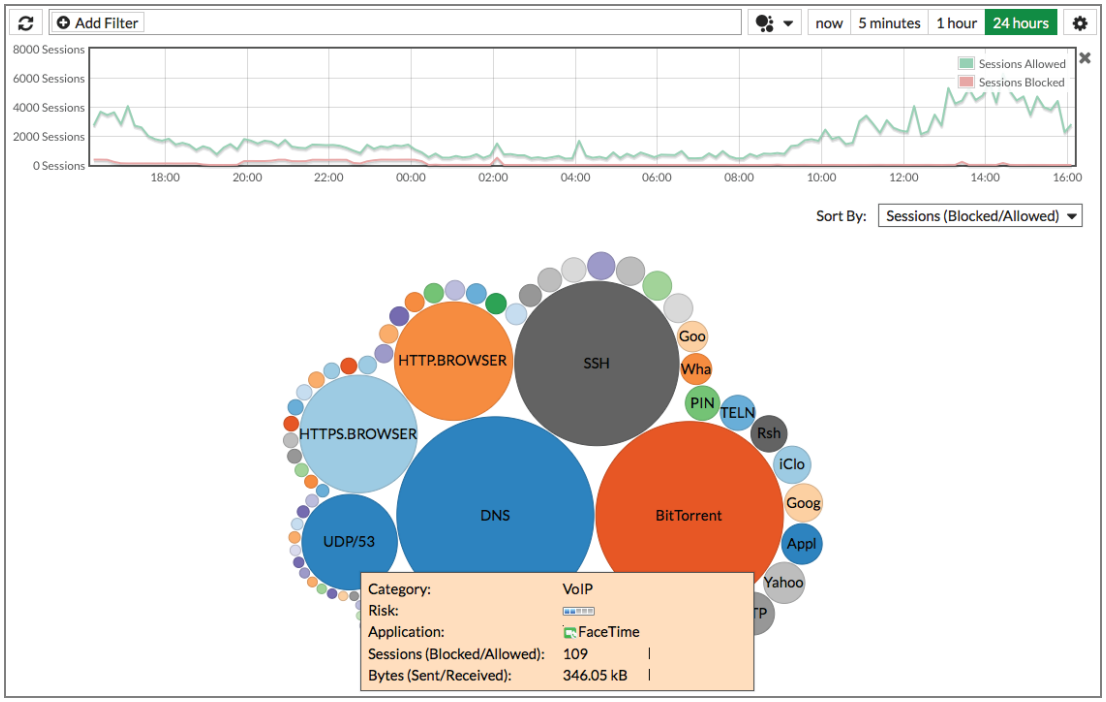
Deep inspection for cloud applications

The prevalence of cloud applications like Dropbox poses a security challenge to today's organizations. Using FortiOS's deep inspection for popular cloud applications, administrators gain deep and useful insights, via FortiView and logs, into activities associated with these applications, such as user IDs, cloud actions, file names, and file sizes. For popular video sites, FortiOS will also be able to track video files viewed.

SSL inspection for encrypted traffic

SSL (Secure Sockets Layer) is a popular encryption standard used to protect Internet traffic but may also be used to evade traditional inspection. FortiOS enables organizations to adopt effective application control even when traffic is encrypted.

Unique hardware components and software optimizations can decrypt traffic with minimal performance impact. The inspection can easily omit sensitive communications, such as financial transaction (thereby complying with privacy policies), or bypass applications that forbid SSL inspection by using granular policy settings.



Monitoring, logging, and reporting

FortiOS empowers organization to implement security best practices that require continuous examination of threat statuses and the ability to adapt to new requirements.

The FortiView widgets provide useful analyses with detailed and contextual session information that can be filtered, ranked, and further inspected. For example, an administrator can instantly query the top applications that are currently consuming bandwidth and drill down to identify their users and help decide if such activities should be blocked.

Network, threat, and system events activities can be archived via syslogs. In turn, these logs can generate useful trending and overview reports.

Lastly, the FortiOS offers robust in-built email and SMS alert systems. Meanwhile, integration with external threat management systems can be achieved with SNMP and standard-based syslogs.

Recipes

Visit cookbook.fortinet.com for these and other recipes:

- NGFW policy-based mode

Inside FortiOS: Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

World class next generation IPS capabilities

Today, sophisticated and high volume attacks are the challenges that every organization must recognize. These attacks are evolving, infiltrating ever-increasing vectors and complex network environments. The result is an urgent need for network protection while maintaining the ability to efficiently provide demanding services and applications.

FortiOS's IPS functionality is an industry-proven network security solution that scales up to over 200 Gbps of in-line protection. Powered by purpose-built hardware and FortiASICs, FortiOS is able to achieve attractive TCO while meeting performance requirements. IPS is easy to set up, yet offers feature-rich capabilities, with contextual visibility and coverage. It is kept up-to-date by research teams that work 24 hours a day worldwide, in order to detect and deter the latest known threats as well as zero-day attacks.

Highlights

- Validated best-in-class security and capacity with proven coverage and high performance.
- Comprehensive protection provided by a signatures-based IPS engine, protocol anomaly scanning, and DDOS mitigation.
- Flexible deployment options and actionable implementations for a wide array of network integration and operation requirements.

Key features & benefits

High Performance IPS, powered by FortiASIC	Low latency and high capacity ensure business applications are not affected while security is enforced.
Best-in-class security with superior coverage	Protects critical digital resources from both internal exploits and external cybercriminals, even if sophisticated attacks are crafted.
Backed by FortiGuard Labs that deliver real-time protection	Maintains up-to-date and proactive protection against latest known threats and newly discovered hacking techniques while allowing time for organizations to patch vulnerable systems.

Features

Tested and proven protection

Not only have FortiGates been deployed in some of the largest enterprises in the world since 2002, FortiOS IPS components and FortiGuard IPS signatures are periodically tested and certified by well-known external labs. For example, Fortinet's FortiGate 3000D earned the highest ratings for Security Effectiveness, blocking 99.9 percent of exploits in the recent NSS Labs DCIPS test. These independent certifications ensure that solutions delivered to customers are of the highest standards in performance, coverage, and accuracy.

Real-time & zero-day protection

The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

FortiGuard IPS service quick facts

- Over 10,000 signatures consisting of 18,000 rules
- Approximately 470,000 network intrusion attempts resisted per minute
- About 1,000 rules are updated or added per week
- Over 300 Zero-day vulnerabilities discovered to date

This update service is backed by a team of threat experts and a close relationship with major application vendors. The best-in-class team also uncovers significant zero-day vulnerabilities continuously, providing FortiGate units with advanced protection ahead of vendor patches.

Uncompromised performance

The FortiASICS Content Processor (CP) accelerates content processing, which is traditionally done completely by the CPU. The CP reduces the resources required by the CPU when matching an incoming file against the signature database, thus improving system performance and stability.

Protocol decoders and anomaly detection

Protocol decoders are required to assemble the packets and detect suspicious, nonconforming sessions that resemble known attacks or are non-compliant to RFC or standard implementation.

FortiOS offers one of the most comprehensive arrays of protocol decoders in the industry, providing customers with significantly wide coverage in all kinds of environments.

Pattern & rate-based signatures

The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiOS offers administrators robust pattern signature selection using filters based on severity, target,

operating system, application, and protocol. Each of the 10,000+ signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. After selection, administrators are able to assign associated actions such as monitoring, blocking, or resetting the session.

Rate-based IPS signatures protect networks against application based DoS and brute force attacks. Administrators can configure nearly 30 rate-based IPS signatures and tune them to their needs. Threshold (incidents per minute) and an action to take when the threshold is reached can be assigned to each signature. If the action is set to block, then a timeout period can be set so that the block is removed after a specified duration.

DoS and DDoS mitigation

DoS policies can help protect against DDoS attacks that aim to overwhelm server resources. In FortiOS, the DoS scans precede the policy engine at the incoming interfaces, thus eliminating unnecessary sessions from the firewall process and state table entry during a surge of attack traffic. This helps to safeguard the firewall from overloading and allows it to perform optimally.

FortiOS DoS policies can be configured to detect and block floodings, port scans, and sweeps. Administrators can set baselines for the amount of concurrent sessions from sources or to destinations. The settings utilize thresholds and can be applied to UDP, TCP, ICMP, IP, and SCTP.

Network interfaces associated with a port attached to a Network Processor (NP) can be configured to offload anomaly checking, further offloading the CPU for greater performance. Some of the anomaly traffic dropped includes LAND attacks, IP protocol with malformed options, and WinNukes.

Quarantine attacks

FortiOS offers sophisticated automatic attack quarantine capabilities which allow organizations to proactively prevent further attacks from known attackers over a predefined duration. Quarantining by duration can be used to protect potentially vulnerable servers until more permanent defense.

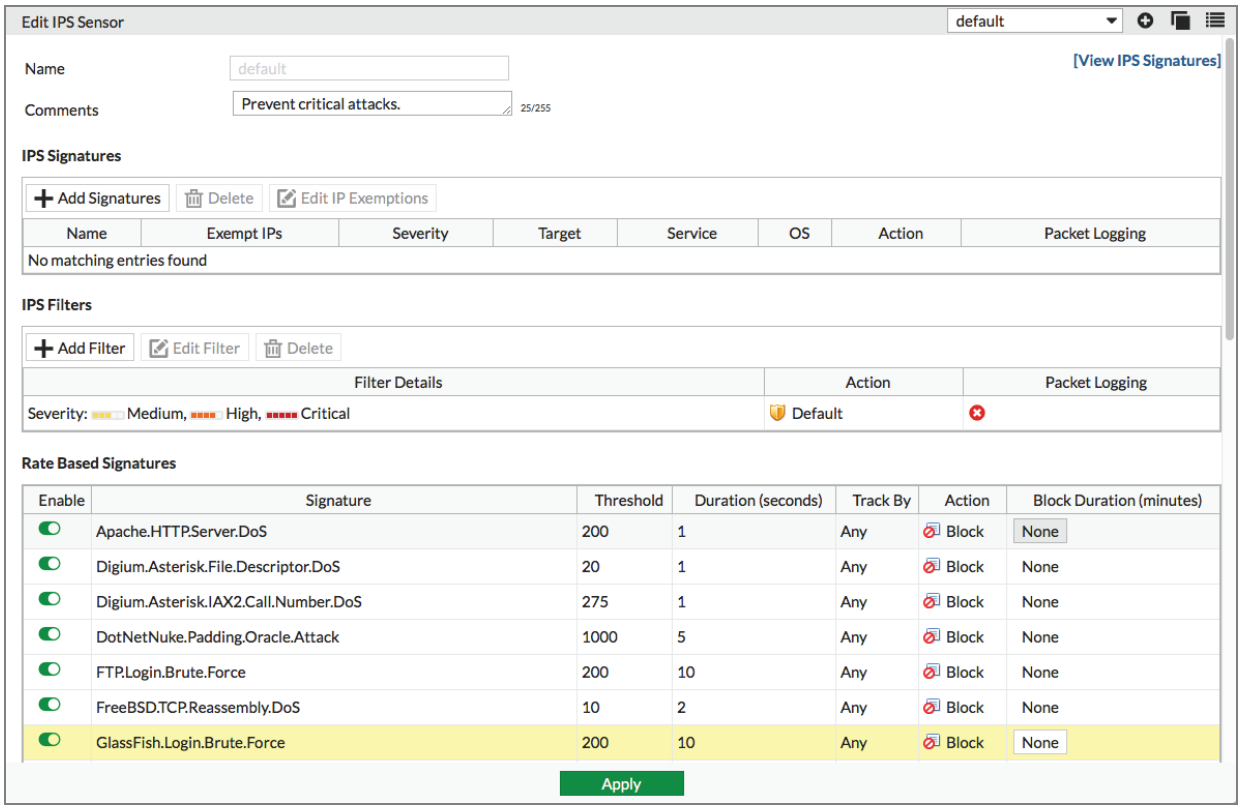
Packet logging

Administrators may choose to automatically perform IPS packet logging, which saves packets for detailed analysis when an IPS signature is matched. Saved packets can be viewed and analyzed on the FortiGate unit or by using third-party analysis tools. Packet logging is also useful in determining false positives.

Custom signatures

Custom IPS signatures can be created to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications, or even custom platforms from known and unknown attacks.

Organizations may use FortiConverter to easily convert Snort signatures for FortiOS use.



Resistant against evasions

Evasion techniques attempt to fool the protocol decoders in IPS products by crafting exotic network streams that would not be handled or reconstructed by the decoders, yet still be valid enough for the target recipient to process. Robust IPS engine is capable of handling both common evasions and sophisticated AETs (Advanced Evasion Techniques) deployed by hackers such as IP Packet Fragmentation, TCP Stream Segmentation, RPC Fragmentation, URL & HTML Obfuscation, and other protocol specific evasion techniques.

Intrusion detection mode

In out-of-band sniffer mode (or one-arm IPS mode), IPS operates as an Intrusion Detection System (IDS), detecting attacks and reporting them but not taking any action against them. In sniffer mode, the FortiGate unit does not process network traffic and instead is connected to a spanning or mirrored switch port, or a network tap. If an attack is detected, log messages can be recorded and alerts sent to system administrators.

Traffic bypass

Since most IPS deployments are in transparent inline mode, active traffic bypass is often desired until normal operation of the device resumes. Some FortiGates offer inbuilt active bypass interfaces while others may use external bypass devices such as the FortiBridge. Administrators are also offered with software fail-open option to tackle instances where the IPS engine fails.

Monitoring, logging, and reporting

FortiOS empowers organizations to implement security best practices that require continuous examination of their threat status and adaptation to new requirements. The FortiView query widgets provide useful analysis data with detailed and contextual session information, which can be filtered, ranked, and further inspected. System events can also be archived via logs, which in turn can generate useful trending and overview reports.

Inside FortiOS: Web Filtering

A Web Filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the Web browser. It may be used to improve security, prevent objectionable activities, and increase productive within an organization.

Intelligent and effective content control

Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more sophisticated and scrutinized than ever, and as well as increasingly difficult to control due to the rise of mobility in the workplace, even more difficult for you to control. The Web has become the preferred medium of choice for hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain. In addition, employees who visit websites containing objectionable content can expose your organization to civil or criminal liability.

FortiOS Web Filtering solution utilizes three main components of the web filtering function: the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service. These functions integrate with each other to provide maximum control over what the Internet user can view as well as protection to the network from many Internet content threats. Web Content Filtering blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic by independent real-world tests.

Highlights

- Comprehensive and advanced Web Filtering features Safe Search and user override options.
- FortiGuard Web Filtering Services with superior coverage of over 250 million rated websites.
- Integration with other FortiOS components, such as User Identification for flexible and secured implementation.
- Supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).
- Ability to configure web filtering by adding URL categories to security policies when operating in flow-based inspection and NGFW policy-based mode. You can set the action to accept or deny to allow or block the applications.

Key features & benefits

Cloud-based Rating Database	Real-time website category rating provides accurate content control.
Wide choice of web filtering technologies	Various web filtering technology options are available to provide each organization the most suitable implementation.
Integrated with other security and networking functions	Allows organizations to simplified networks and reduce TCO.

Features

Cloud-based rating system

Fortinet is a pioneer in cloud-based rating systems for web filtering. FortiOS provides an innovative approach to HTTP and HTTPS web filtering technology by combining the advantages of a cloud-based service offering with layered response caching. The multiple FortiGuard data centers around the world hold the entire categorized URL database and receive rating requests from FortiGate units triggered by browser-based URL requests. FortiGuard responds to these rating requests with the categories stored for specific URLs, the requesting FortiGate unit then uses its own local profile configuration to determine what action is appropriate to the category, such as: blocking, monitoring, allowing the page, displaying a warning, or requiring authentication to view the page.

Rating responses are also cached directly in FortiGate unit memory so that ratings for frequently used sites can be retrieved directly from the cache, reducing the number of requests to the FortiGuard network. Caching URLs in memory makes URL lookups almost instantaneous while only using a very small amount of system memory.

An appropriately licensed FortiManager appliance can be synchronized to the FortiGuard network and as such can be used in the same way to as the FortiGuard network for managed FortiGate devices. This can further reduce any latency associated with the round trip time for individual rating requests while at the same time ensuring complete database coverage. Consider the combination of a LAN attached FortiGate cluster and FortiManager combination with the potential to handle tens of thousands of requests per second.

Superior coverage

FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. This service currently rates more than 250 million sites covering billions of URLs with each site able to be rated in multiple categories. The FortiGuard database provides a truly international service with support for 70 languages.

Extensive and flexible categorization

Rated URLs are assigned into one of the 98 categories (including 20 user defined ones) which administrators can then easily manage and control. Administrators can configure and populate local categories or place specific URLs in existing categories should the FortiGuard rating not be in agreement with an organization’s policies and practices.

Rating override

At times, administrators may have to allow approved people to access what they need during periods when an exception to the normal rules is required, while still having enough control that the organization’s web usage policies are not compromised. FortiOS can provide such setup by using alternate profiles.

Protection against malicious URLs

The malicious URL database contains all malicious URLs active in the last month and is organized as one of the categories. With Fortinet Security Fabric, customers can further their protection by having the FortiSandbox add

newly discovered URLs to a dynamic URL filter, thus blocking files from being downloaded again from that URL.

Inspection modes

FortiOS web filtering can operate in different modes: proxy-based and flow-based inspection modes and DNS filtering. Each mode has strengths and weaknesses and all three can be active at the same time on different traffic streams.

Proxy-based web filtering uses a proxy to assemble and analyze web content as it passes through the FortiGate unit. If a page is blocked the proxy can replace the blocked page with a customizable web page informing users that the page is blocked. Proxy-based web filtering is the most feature-rich mode, supporting many advanced filters including web content filtering that analyzes web page content according to your custom requirements, Java applet filtering, and blocking invalid URLs.

Flow-based web filtering uses the FortiOS IPS engine to filter web content packets as they pass through the FortiGate unit without any buffering. Flow-based inspection does not use a proxy, so inspected packets are not proxied and altered by the FortiGate unit. Flow-based inspection does not support as many advanced features as proxy-based web filtering.

To control your FortiGate's security profile inspection mode in FortiOS 5.6, you can select **Flow** or **Proxy Inspection Mode** from **System > Settings**. Having control over flow and proxy mode is helpful if you want to ensure that only flow inspection mode is used.

In most cases proxy mode is preferred because more security profile features are available and more configuration options for these individual features are available. Some implementations, however, may require all security profile scanning to only use flow mode. In this case, you can set your FortiGate to flow mode knowing that proxy mode inspection will not be used.

Two new policy modes are available in FortiOS 5.6.

- NGFW mode simplifies applying application control and web filtering to traffic by allowing you to add applications and web filtering profiles directly to policies. This is used in conjunction with flow-based inspection.
- Transparent proxy allows you to apply web authentication to HTTP traffic without using the explicit proxy.

DNS web filtering employs DNS lookups to the FortiGuard DNS service to get web page ratings. Filtering is done as part of the DNS lookup and web pages can be blocked or redirected to a web filter block page before the HTTP session starts. As a result, it is lightweight in terms of resource usage although it only supports a limited number of advanced features.

Usage quota

Administrators can set a daily timed access quota by category or category group. Quotas allow access for a specified length of time or traffic volume, calculated separately for each user.

SafeSearch

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch on the FortiGate for the supported search sites can better enforce its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature.

Restrict YouTube access

In FortiOS 5.6 with inspection mode set to proxy-based, you can set Strict or Moderate access to YouTube in a Web Filter profile.

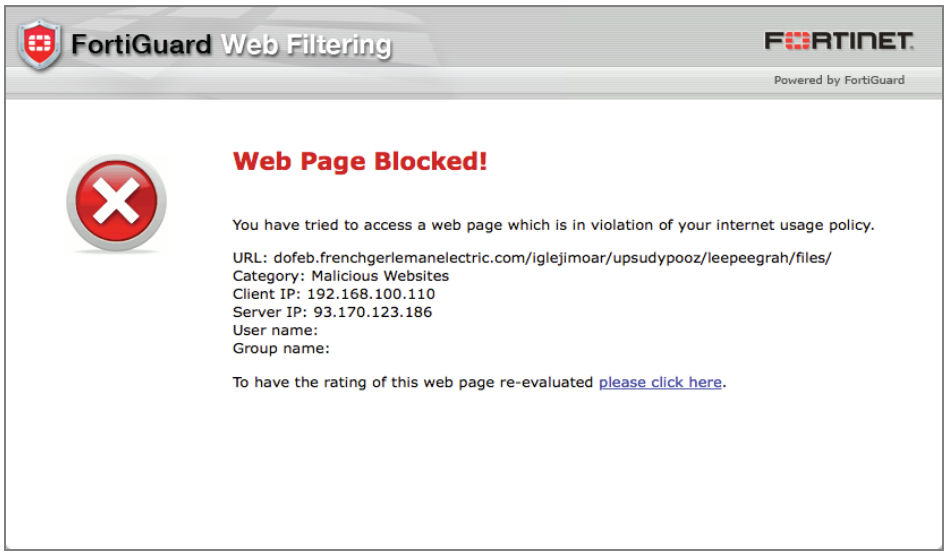
Manual URL and content filter

FortiOS web filtering offers specific URL filtering by standard, wildcard, and regular expression definition, as well as content filtering by pattern type and language.

Advanced web filter configurations

FortiOS rich feature set includes ability to implement a number of enterprise features such as:

- Block HTTP redirects by rating, invalid URLs, HTTP POST actions, and Web resume download
- Cookie, Java applet, and ActiveX filter
- Rate Images by URL and URLs by domain and IP address
- Restrict Google account usage to specific domains



Proxy avoidance preventions

FortiGate is able to improve the effectiveness of the web filtering by preventing users from evading the security implementation. Organizations can use its multiple integrated technologies including proxy site URL, proxy application control, and IPS proxy behavior blocking.

User and device awareness

Most networks in today's organizations are connected with both corporate and personal mobile devices. User and device awareness provides the option to configure intelligent policies that can effectively enforce security.

To tackle the prevalence of BYOD environments, administrators are able to configure web content access policies with sources defined by IPs, users, and devices, either combined or selectively.

External URL filtering support

In instances where customers have large, existing, deployed implementations of a specific URL filtering solution but replace their legacy firewalls with a FortiGate family, they can still retain their web filtering infrastructure since FortiOS supports both ICAP and WISP.

Monitoring, logging, and reporting

FortiOS empowers an organization to implement security best practices that require continuous monitoring of threats, allowing the organization to adapt to new requirements.

The FortiView dashboards display useful analysis data with detailed and contextual session information, which can be filtered and ranked, with drilldown options also available. This information, including system events activities and administration audit trails, can also be archived via logs.

FortiOS logs all the types of traffic that can connect to or terminate at the FortiGate unit. In turn, these logs can generate useful trending and overview reports.

Security profiles overview

The FortiGate line combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as Security Profiles.

This overview addresses the following topics:

- Traffic inspection
- Content inspection and filtering
- Security profile components
- Security profiles/lists/sensors

Firewall policies limit access, and while this and similar features are a vital part of securing your network, they are not covered in this discussion of Security Profiles.

FortiOS 5.4 no longer supports FortiClient 5.0.

FortiOS 5.4.1 supports only FortiClient 5.4.1. Be sure to upgrade managed FortiClients before upgrading the FortiGate to 5.4.1.

FortiOS 5.2 can support FortiClient 5.0, but only if the FortiGate upgraded to FortiOS 5.2. Customers need to purchase a FortiClient 5.4 subscription-based FortiClient license.

Traffic inspection

When the FortiGate unit examines network traffic one packet at a time for IPS signatures, it is performing traffic analysis. This is unlike content analysis where the traffic is buffered until files, email messages, web pages, and other files are assembled and examined as a whole.

DoS policies use traffic analysis by keeping track of the type and quantity of packets, as well as their source and destination addresses.

Application control uses traffic analysis to determine which application generated the packet.

Although traffic inspection doesn't involve taking packets and assembling files they are carrying, the packets themselves can be split into fragments as they pass from network to network. These fragments are reassembled by the FortiGate unit before examination.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against content threats.

IPS signatures

IPS signatures can detect malicious network traffic. For example, the Code Red worm attacked a vulnerability in the Microsoft IIS web server. Your FortiGate's IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions.

IPS recommendations

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive new IPS signatures as soon as they are available.
- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to **Block**.
- You can view these signatures by going to **Security Profiles > Intrusion Prevention** and selecting the **[View IPS Signatures]** link in the right-hand corner of the window.
- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to **Block**.

Suspicious traffic attributes

Network traffic itself can be used as an attack vector or a means to probe a network before an attack. For example, SYN and FIN flags should never appear together in the same TCP packet. The SYN flag is used to initiate a TCP session while the FIN flag indicates the end of data transmission at the end of a TCP session.

The FortiGate unit has IPS signatures that recognize abnormal and suspicious traffic attributes. The SYN/FIN combination is one of the suspicious flag combinations detected in TCP traffic by the `TCP.BAD.FLAGS` signature.

The signatures that are created specifically to examine traffic options and settings, begin with the name of the traffic type they are associated with. For example, signatures created to examine TCP traffic have signature names starting with TCP.

Application control

While applications can often be blocked by the ports they use, application control allows convenient management of all supported applications, including those that do not use set ports.

Application control recommendations

- Some applications behave in an unusual manner in regards to application control. For more information, see Application considerations on page 129.
- By default, application control allows the applications not specified in the application control list. For high security networks, you may want to change this behavior so that only the explicitly allowed applications are permitted.

SSL/SSH inspection

Regular web filtering can be circumvented by using https:// instead of http://. By enabling this feature, the FortiGate can filter traffic that is using the HTTPS protocol. This sort of analysis is some times referred to as deep scanning.

Deep Inspection works along the following lines: If your FortiGate unit has the correct chipset it will be able to scan SSL encrypted traffic in the same way that regular traffic can be scanned. The FortiGate firewall will essentially receive the traffic on behalf of the client and open up the encrypted traffic. Once it is finished it re-

encrypts the traffic and sends it on to its intended recipient. It is very similar to a man-in-the-middle attack. By enabling this feature, it allows the FortiGate firewall to filter on traffic that is using the SSL encrypted protocol.

The encrypted protocols that can be inspected are:

- HTTPS
- SMTPS
- POP3S
- IMAPS
- FTPS

Before the invention of SSL inspection, scanning regular web traffic can be circumvented by using the prefix https:// instead of http:// in the URL. SSL inspection prevents this circumvention. However, because when the encrypted traffic is decrypted it has to be re-encrypted with the FortiGate's certificate rather than the original certificate it can cause errors because the name on the certificate does not match the name on the web site.

At one point deep inspection was something that was either turned on or off. Now individual deep inspection profiles can be created depending on the requirements of the policy. Depending on the Inspection Profile, you can:

- Configure which CA certificate will be used to decrypt the SSL encrypted traffic.
- Configure which SSL protocols will be inspected.
- Configure which ports will be associated with which SSL protocols for the purpose of inspection.
- Configure which websites will be exempt from SSL inspection
- Configure whether or not to allow invalid SSL certificates.
- Configure whether or not SSH traffic will be inspected.

Web rating overrides

This feature allows you to override the FortiGuard Web Filtering. This option allows users to change the rating for a website and control access to the site without affecting the rest of the sites in the original category. More information can be found in Overriding FortiGuard website categorization.

Web profile overrides

This feature allows administrators to grant temporary access to sites that are otherwise blocked by a web filter profile. The temporary access can be granted to a user, user group, or source IP address. The time limit can be set in days, hours, or minutes. See the section on Web Profile Overrides for more information.

Content inspection and filtering

When the FortiGate unit buffers the packets containing files, email messages, web pages, and other similar files for reassembly before examining them, it is performing content inspection. Traffic inspection, on the other hand, is accomplished by the FortiGate unit examining individual packets of network traffic as they are received.

No two networks are the same and few recommendations apply to all networks. This topic offers suggestions on how you can use the FortiGate unit to help secure your network against threats to content. Be sure to understand the effects of the changes before using the suggestions.

AntiVirus

The FortiGate antivirus scanner can detect viruses and other malicious payloads used to infect machines. The FortiGate unit performs deep content inspection. To prevent attempts to disguise viruses, the antivirus scanner will reassemble fragmented files and uncompress content that has been compressed. Patented Compact Pattern Recognition Language (CPRL) allows further inspection for common patterns, increasing detection rates of virus variations in the future.

AntiVirus recommendations

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure that new antivirus signatures are loaded onto your FortiGate as soon as they are available.
- Enable the Extended Virus Database if your FortiGate unit supports it.
- Examine antivirus logs periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.
- To conserve system resources, avoid scanning email messages twice. Scan messages as they enter and leave your network or when clients send and retrieve them, rather than both.
- Enable **Treat Windows Executables in Email Attachments as Viruses** if you are concerned about incoming '.exe' files.

FortiGuard web filtering

The web is the most popular part of the Internet and, as a consequence, virtually every computer connected to the Internet is able to communicate using port 80, HTTP. Botnet communications take advantage of this open port and use it to communicate with infected computers. FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.

FortiGuard web filtering recommendations

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous.
- In the Anti-Spam profile, enable **Spam Detection and Filtering** and then enable **IP Address Check**. Many IP addresses used in spam messages lead to malicious sites; checking them will protect your users and your network.

DNS filter

DNS-based web filtering

This feature is similar to the FortiGuard DNS web filtering available in FortiOS 5.2. You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiGate must use the FortiGuard DNS service for DNS lookups. DNS lookup requests

sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

If that FortiGuard category is set to block, the result of the DNS lookup is not returned to the requester. If the category is set to redirect, then the address returned to the requester points at a FortiGuard redirect page.

You can also allow access or monitor access based on FortiGuard category.

The following filtering options can be configured in a DNS Filter security profile:

Blocking DNS requests to known Botnet C&C addresses

A new FortiGuard database contains a list of known Botnet C&C addresses. This database is updated dynamically and stored on the FortiGate. This database is covered by FortiGuard web filter licensing; you must have an active FortiGuard web filtering license to use this feature. You can view the botnet lists by going to **System > FortiGuard > Botnet IPs** and **System > FortiGuard > Botnet Domains**.

When you block DNS requests to known Botnet C&C addresses, using IPS, DNS lookups are checked against the Botnet C&C database. All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all sub-domains are also blocked.

To enable blocking of DNS requests to known Botnet C&C addresses, go to **Security Profiles > DNS Filter**, and enable **Block DNS requests to known botnet C&C**. When you do this in FortiOS 5.4.1, you can open a definitions window by clicking on "botnet package."

Static URL filter

The DNS static URL filter allows you to block, exempt, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match the DNS request can be blocked, exempted, monitored, or allowed.

If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site.

If exempted, access to the site is allowed even if another method is used to block it.

Anti-Spam

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine. The FortiGate email filter can detect harmful spam and mark it, alerting the user to the potential danger.

Anti-Spam filter recommendations

- Subscribe to the FortiGuard Anti-Spam Filtering service.
- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint scanning for protection against threats that get into your network.

Data Leak Prevention

Most security features on the FortiGate unit are designed to keep unwanted traffic out of your network while Data Leak Prevention (DLP) can help you keep sensitive information from leaving your network. For example, credit card numbers and social security numbers can be detected by DLP sensors.

DLP recommendations

- Rules related to HTTP posts can be created, but if the requirement is to block all HTTP posts, a better solution is to use application control or the **HTTP POST Action** option in the web filter profile.
- While DLP can detect sensitive data, it is more efficient to block unnecessary communication channels than to use DLP to examine it. If you don't use instant messaging or peer-to-peer communication in your organization, for example, use application control to block them entirely.

Security profile components

Below is a brief description of the security profiles and their features.

Security Profiles can be configured Globally across multiple VDOMs. See "Global security profiles across Virtual domains (VDOMs)" on page 230 for more information.

AntiVirus

Your FortiGate unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support additional virus databases are able to identify hundreds of thousands of viruses. With a FortiGuard AntiVirus subscription, the signature databases are updated whenever a new threat is discovered.

AntiVirus also includes file filtering. When you specify files by type or by file name, the FortiGate unit will block the matching files from reaching your users.

FortiGate units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files for that you can examine later.

Web filter

Web filtering includes a number of features you can use to protect or limit your users' activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

DNS filter

The FortiGate will inspect DNS traffic to any DNS server, so long as the policy has DNS inspection enabled. The FortiGate will intercept DNS requests, regardless of the destination IP, and redirect it to the FortiGuard Secure

DNS server -- this is separate from the FortiGuard DNS server.

The Secure DNS server will resolve and rate the FQDN and send a DNS response which includes both IP and rating of the FQDN back to the FortiGate, where it will handle the DNS response according to the DNS filter profile.

Application control

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1,000 applications, improving your control over application communication.

Cloud Access Security Inspection (CASI)

This feature introduces a new security profile called Cloud Access Security Inspection (CASI) that provides support for fine-grained control on popular cloud applications, such as YouTube, Dropbox, Baidu, and Amazon. The CASI profile is applied to a policy much like any other security profile.

Unfortunately CASI does not work when using Proxy-based profiles for AV or Web filtering for example.
Make sure to only use Flow-based profiles in combination with CASI on a specific policy.

Intrusion protection

The FortiGate Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures tailored to your network.

Anti-spam

FortiGuard Anti-Spam is a subscription service that includes an IP address black list, a URL black list, and an email checksum database. These resources are updated whenever new spam messages are received, so you do not need to maintain any lists or databases to ensure accurate spam detection.

You can use your own IP address lists and email address lists to allow or deny addresses, based on your own needs and circumstances.

Data Leak Prevention

Data Leak Prevention (DLP) allows you to define the format of sensitive data. The FortiGate unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.

VoIP

The Session Initiation Protocol (SIP) is an IETF application layer signaling protocol used for establishing, conducting, and terminating multi-user multimedia sessions over TCP/IP networks using any media. SIP is often used for Voice over IP (VoIP) calls but can be used for establishing streaming communication between end points.

For more information, see VoIP Solutions: SIP.

ICAP

This module allows for the offloading of certain processes to a separate server so that your FortiGate firewall can optimize its resources and maintain the best level of performance possible.

FortiClient profiles

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

The FortiGate provides network security by defining compliance rules for FortiClient endpoints.

For more information, see the FortiClient 5.4.1 Administration Guide.

Proxy options

Proxy Options includes features you can configure for when your FortiGate is operating in proxy mode, including protocol port mapping, block oversized files/emails, and other web and email options.

SSL/SSH inspection

SSL/SSH Inspection (otherwise known as Deep Inspection) is used to scan HTTPS traffic in the same way that HTTP traffic can be scanned. This allows the FortiGate to receive and open up the encrypted traffic on behalf of the client, then the traffic is re-encrypted and sent on to its intended destination.

Individual Deep Inspection profiles can be created, depending on the requirements of the policy. Depending on the profile, you can:

- Configure which CA certificate will be used to decrypt the SSL encrypted traffic
- Configure which SSL protocols will be inspected
- Configure which ports will be associated with which SSL protocols for inspection
- Configure whether or not to allow invalid SSL certificates
- Configure whether or not SSH traffic will be inspected

Security profiles/lists/sensors

A profile is a group of settings that you can apply to one or more firewall policies. Each Security Profile feature is enabled and configured in a profile, list, or sensor. These are then selected in a security policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the security policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

While you can apply more than one security profile to a firewall policy, it is not recommended that you use flow-based profiles and proxy-based profiles in the same firewall policy.

Because you can use profiles in more than one security policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks.

Inspection modes

You can select one of two inspection modes from the **System > Settings** page to control the security profile inspection mode for your FortiGate or VDOM.

- Proxy-based inspection, that reconstructs content passing through the FortiGate unit and inspects the content for security threats, or
- Flow-based inspection, that takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

Each inspection component plays a role in the processing of traffic en route to its destination. Having control over flow and proxy mode is helpful if you want to be sure that only flow inspection mode is used (and that proxy inspection mode is not used). In most cases proxy mode is preferred because more security profile features are available and more configuration options for these individual features are available. Yet, some implementations may require all security profile scanning to only use flow mode. In this case, you can set your FortiGate to flow mode knowing that proxy mode inspection will not be used. While both modes offer significant security, proxy-based provides more features and flow-based is designed to optimize performance.

This section addresses the following topics:

Proxy-based inspection

If a FortiGate or VDOM is configured for proxy-based inspection, then a mixture of flow-based and proxy-based inspection occurs. Traffic initially encounters the IPS engine, which applies single-pass IPS, Application Control, and CASI, if configured in the firewall policy accepting the traffic.

The traffic is then sent for proxy-based inspection. Proxy-based inspection extracts and caches content, such as files and web pages, from a content session and inspects the cached content for threats. Content inspection takes place in the following order: **VoIP inspection**, **DLP**, **AntiSpam**, **Web Filtering**, **AntiVirus**, and **ICAP**.

If no threat is found, the proxy relays the content to its destination. If a threat is found, the proxy can block the threat and send a replacement message in its stead. The proxy can also block VoIP traffic that contains threats.

Transparent web proxy mode

In proxy mode, FortiOS 5.6 functions just like FortiOS 5.4 with the addition of the new Transparent Web Proxy mode. See New Operating mode for Transparent web proxy in What's New in FortiOS 5.6.

Flow-based inspection

Flow-based inspection identifies and blocks security threats in real time as they are identified using single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats.

If a FortiGate or a VDOM is configured for flow-based inspection, depending on the options selected in the firewall policy that accepted the session, flow-based inspection can apply **IPS**, **Application Control**, **Web Filtering**, **DLP**, and **AntiVirus**. Flow-based inspection is all done by the IPS engine and, as you would expect, no proxying is involved.

All of the applicable flow-based security modules are applied simultaneously in one single pass, and pattern matching is offloaded and accelerated by CP8 or CP9 processors. **IPS**, **Application Control**, flow-based **Web Filtering**, and flow-based **DLP** filtering happen together. Flow-based **AntiVirus** scanning caches files during protocol decoding and submits cached files for virus scanning while the other matching is carried out.

Flow-based inspection typically requires fewer processing resources than proxy-based inspection and does not change packets, unless a threat is found and packets are blocked. Flow-based inspection cannot apply as many features as proxy inspection. For example, flow-based inspection does not support client comforting and some aspects of replacement messages.

In FortiOS 5.6, flow-based inspection requires the new NGFW mode.

Changing between proxy and flow mode

You can see which inspection mode your FortiGate is using by looking at the **System Information** widget on your **Dashboard**.

To change inspection modes, go to **System > Settings** and scroll down to **Inspection Mode**. You can select Flow-based to operate in Flow mode or Proxy to operate in Proxy mode.

When you select **Flow-based**, all proxy mode profiles are converted to flow mode, removing any proxy settings. As well proxy mode only features (for example, Web Application Profile) are removed from the GUI.

In addition, selecting **Flow-based** inspection will cause the **Explicit Web Proxy** and **Explicit FTP Proxy** features to be removed from the GUI and the CLI. This includes Explicit Proxy firewall policies.

W hen you select **Flow-based** you can only configure Virtual Servers (under **Policy & Objects > Virtual Servers**) with Type set to HTTP, TCP, UDP, or IP.

If required, you can change back to proxy mode through the **System > Settings** page.

If your FortiGate has multiple VDOMs, you can set the inspection mode independently for each VDOM. Use the top left drop-down menu to go to **Global > System > VDOM**. Click **Edit**for the VDOM you wish to change and select the **Inspection Mode**.

Switching to flow-based inspection also turns off WAN Optimization, Web Caching, the Explicit Web Proxy, and the Explicit FTP Proxy making sure that no proxying can occur.

From the GUI, you can only configure antivirus and web filter security profiles in proxy mode. From the CLI you can configure flow-based antivirus profiles, web filter profiles and DLP profiles and they will appear on the GUI and include their inspection mode setting. Also, flow-based profiles created when in flow mode are still available when you switch to proxy mode.

NGFW profile-based and NGFW policy-based modes

When you select **Flow-based** as the **Inspection Mode**, you have the option in FortiOS 5.6 to select an **NGFW Mode**. **NGFW Profile-based** mode works the same as flow-based mode did in FortiOS 5.4

When selecting NGFW policy-based mode you can also select the SSL/SSH Inspection mode that is applied to all policies.

In the new **NGFW Policy-based** mode, you add applications and web filtering profiles directly to a policy without having to first create and configure Application Control or Web Filtering profiles. See NGFW Policy Mode on page 1.

When you change to flow-based inspection, all proxy mode profiles are converted to flow mode, removing any proxy settings. And proxy-mode only features (for example, Web Application Profile) are removed from the GUI.

If your FortiGate has multiple VDOMs, you can set the inspection mode independently for each VDOM. Go to **System > VDOM**. Click **Edit** for the VDOM you wish to change and select the **Inspection Mode**.

CLI syntax

The following CLI commands can be used to configure inspection and NGFW (called "policy" in the CLI) modes:

```
config system settings
   set inspection-mode {proxy | flow}
   set policy-mode {standard | ngfw}
end
```

Comparison of inspection types

The tables in this section show how different security features map to different inspection types and present the strengths and weaknesses of proxy- vs. flow-based inspection.

Security profile features mapped to inspection mode

The table below lists FortiOS security profile features and shows whether they are available in flow-based or proxy-based inspection modes.

Security Profile Feature	Flow-based inspection	Proxy-based inspection
AntiVirus	x	x
Web Filter	x	x

Security Profile Feature	Flow-based inspection	Proxy-based inspection
DNS Filter	x	x
Application Control	x	x
Intrusion Protection	x	x
Anti-Spam		x
Data Leak Protection		x
VoIP		x
ICAP		x
Web Application Firewall		x
FortiClient Profiles	x	x
Proxy Options	x	x
SSL Inspection	x	x
SSH Inspection		x
Web Rating Overrides	x	x
Web Profile Overrides		x

Individual security profile considerations

In flow mode, AntiVirus and Web Filter profiles only include flow-mode features. Web filtering and virus scanning are still done with the same engines and to the same accuracy, but some inspection options are limited or not available in flow mode. Application control, intrusion protection, and FortiClient profiles are not affected when switching between flow and proxy mode.

Application control uses flow-based inspection; if you apply an additional security profile to your traffic that is proxy-based, the connection will simply timeout rather than display the warning, or replacement, message. However, Application Control will still function.

Even though VoIP profiles are not available from the GUI in flow mode, the FortiGate can process VoIP traffic. In this case the appropriate session helper is used (for example, the SIP session helper).

Setting flow or proxy mode doesn't change the settings available from the CLI. However, when in flow mode you can't save security profiles that are set to proxy mode.

You can also add proxy-only security profiles to firewall policies from the CLI. So, for example, you can add a VoIP profile to a security policy that accepts VoIP traffic. This practice isn't recommended because the setting will not be visible from the GUI.

If you set flow-based to use external servers for FortiWeb and FortiMail you must use the CLI to set a Web Application Firewall profile or Anti-Spam profile to external mode and add the Web Application Firewall profile or AntiSpam profile to a firewall policy.

Proxy mode and flow mode antivirus and web filter profile options

The following tables list the antivirus and web filter profile options available in proxy and flow modes.

Antivirus features in proxy and flow mode

Feature	Proxy	Flow
Scan Mode (Quick or Full)	no	yes
Detect viruses (Block or Monitor)	yes	yes
Inspected protocols	yes	no (all relevant protocols are inspected)
Inspection Options	yes	yes (not available for quick scan mode)
Treat Windows Executables in Email Attachments as Viruses	yes	yes
Send Files to FortiSandbox Appliance for Inspection	yes	yes
Use FortiSandbox Database	yes	yes
Include Mobile Malware Protection	yes	yes

Web filter features in proxy and flow mode

Feature	Proxy	Flow
FortiGuard category based filter	yes	yes (show, allow, monitor, block)
Category Usage Quota	yes	no
Allow users to override blocked categories (on some models)	yes	no
Search Engines	yes	no

Feature		Proxy	Flow
	Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	yes	no
	Restrict YouTube Access	yes	no
	Log all search keywords	yes	no
Static URL Filter		yes	yes
	Block invalid URLs	yes	no
	URL Filter	yes	yes
	Block malicious URLs discovered by FortiSandbox	yes	yes
	Web Content Filter	yes	yes
Rating Options		yes	yes
	Allow websites when a rating error occurs	yes	yes
	Rate URLs by domain and IP Address	yes	yes
	Block HTTP redirects by rating	yes	no
	Rate images by URL	yes	no
Proxy Options		yes	no
	Restrict Google account usage to specific domains	yes	no
	Provide details for blocked HTTP 4xx and 5xx errors	yes	no
	HTTP POST Action	yes	no
	Remove Java Applets	yes	no
	Remove ActiveX	yes	no
	Remove Cookies	yes	no
	Filter Per-User Black/White List	yes	no

AntiVirus scanning differences between versions of FortiOS 5.x

In FortiOS 5.0, 5.2, 5.4, 5.6 and 6.0, there are several AntiVirus (AV) scanning inspection modes available. FortiOS 5.0 includes proxy and flow-based virus scanning. FortiOS 5.2 also uses proxy-based and flow-based scanning, but the flow-based mode in FortiOS 5.2 uses a new approach to flow-based scanning (that is sometimes called deepflow or deep flow scanning). FortiOS 5.4 and onward offer another flow-based mode, quick mode, to inspect traffic efficiently.

The databases used for AV scanning does not change from proxy to flow mode unless quick mode is enabled. In flow-based quick mode, a compact antivirus database is used.

AntiVirus scanning examines files in HTTP, HTTPS, email, and FTP traffic for threats as they pass through your FortiGate. If the traffic contains compressed files, they are also examined. Go to the SysAdmin Note on the Fortinet Cookbook site for detailed information on supported compression formats in antivirus scanning.

If the AV scanner finds a threat such as a virus or some other malware, FortiOS protects your network by blocking the file.

FortiOS includes a number of AntiVirus features that make virus scanning more user-friendly. One of these features, called replacement messages, sends a customizable message to anyone whose file is blocked by AV scanning, to explain what happened and why. Other features make communication between the client and the server more seamless. The availability of these changes depending on the inspection mode.

Proxy-based AV scanning

Proxy-based AV scanning is the most feature-rich AV scanning mode. This mode uses a proxy to manage the communication between client and server. The proxy extracts content packets from the data stream as they arrive and buffers the content until the complete file is assembled. Once the file is whole, the AV scanner examines the file for threats. If no threats are found, the file is sent to its destination. If a threat is found, the file is blocked.

Because proxy-based scanning is applied to complete files, including compressed files, it provides very effective threat detection. Proxy-based scanning also supports a full range of features, including replacement messages and client comforting, making proxy-based scanning the most user friendly inspection mode. In addition the proxy manages the communication between the client and the server, improving the user experience. For example, in flow mode if a virus is found, the last part of the file is not downloaded and the connection just times out and the user cannot tell what is going on. In proxy mode, the users gets a message about the file being blocked.

Proxy-based scanning inspects all files under the oversized threshold. Since the FortiGate unit has a limited amount of memory, files larger than a certain size do not fit within the memory buffer. The default buffer size is 10 MB. You can use the `uncompsizelimit`CLI command to adjust the size of this memory buffer. Files larger than the threshold are passed to the destination without scanning. You can use the **Oversized File/Email** setting in **Security Profiles > Proxy Options** to block files larger than the antivirus buffer if allowing files that are too large to be scanned is an unacceptable security risk.

During the buffering and scanning procedure, the client must wait. With a default configuration, the file is released to the client only after it is scanned. You can enable client comforting in the **Proxy Options** security profile to feed the client a trickle of data to prevent them from possibly thinking the transfer is stalled and consequently canceling the download.

Flow-based AV scanning

Although the name "flow-based scanning" is used in FortiOS 5.0, 5.2, 5.4, and 5.6, the different versions handle this mode in very different ways.

Flow AV in FortiOS 5.4 and 5.6

In FortiOS 5.4 and 5.6, there are two modes available for flow-based virus scanning: **Quick** and **Full** scan mode. Full mode is the same as flow-based scanning in FortiOS 5.2 (see below). Quick mode uses a compact antivirus database and advanced techniques to improve performance. You can designate quick or full scan mode when configuring the antivirus profile in the GUI. Alternatively, use the following CLI command to enable quick or full mode:

```
config antivirus profile
   edit <profile>
      set scan-mode {quick | full}
   end
```

Flow AV in FortiOS 5.2 (deepflow or deep flow)

FortiOS 5.2 introduced a new type of flow-based AV scanning, that is sometimes called deepflow or deep flow, and that takes a hybrid approach where content packets are buffered while simultaneously being sent to their destination. When all of the files packets have been collected and buffered, but before the final packet is delivered, the buffered file is scanned. If a threat is found, the last packet is blocked and the client application has to deal with not getting the completed file. If no threat is found the final packet is sent and the user gets their file.

Deepflow AV scanning is as good as proxy-based AV scanning at detecting threats. There may be a small performance advantage over proxy-based AV as files get larger based on the difference between sending the whole file after analysis and just sending the last packet. Deepflow's most notable limitation is that, just like the flow-based AV in 5.0, it does not support many of the user-friendly features provided by proxy-based AV.

Flow AV in FortiOS 5.0

In FortiOS 5.0, flow-based AV scanning examines the content of individual data packets as they pass through the FortiGate. There is no proxy involved so packets are not changed by the proxy and files are not buffered for analysis. Potentially less memory and CPU resources are used, resulting in a potential performance increase compared to using proxy-based mode. FortiOS 5.0 flow-based AV scanning is also not limited by file size.

Flow AV uses the IPS engine and the AV database and is effective at many kinds of threat detection; however, because it can only analyze what is in an individual packet rather than a complete file, flow-based scanning cannot detect some types of malware, including polymorphic code. Malware in documents, compressed files, and some archives are also less likely to be detected.

Flow AV does not actually block files, it stops delivering a file's packets once a threat has been detected. This means that parts of the file may already have been delivered when the threat has been detected and the recipient application is responsible for dealing with the partially complete content.

In addition flow AV can be less user friendly. Replacement messages are not supported and clients may have to wait for sessions to time out without knowing why content has been blocked.

AntiVirus

This section describes how to configure the antivirus options. From an antivirus profile you can configure the FortiGate unit to apply antivirus protection to HTTP, FTP, IMAP, POP3, SMTP, and NNTP sessions. If your FortiGate unit supports SSL/SSH content scanning and inspection, you can also configure antivirus protection for HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions.

In many cases you can just customize the default antivirus profile and apply it to the security policy that accepts the traffic to be virus scanned. You can also create custom antivirus profiles if want to apply different types of virus protection to different traffic.

This Handbook chapter includes Inside FortiOS: AntiVirus providing readers an overview of the features and benefits of key FortiOS components.

For readers needing to delve into greater detail, we provide the following topics:

- Antivirus concepts
- Enabling AntiVirus scanning
- Testing your antivirus configuration
- Example Scenarios

Antivirus concepts

The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.

The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.

Antivirus scanning examines files for viruses, worms, trojans, and other malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.

Malware threats

Malware is the general term covering all the different types of threats to your computer safety such as:

- Viruses
- Worms
- Trojan horses
- Ransomware
- Scareware
- Spyware

- Adware
- Botnets
- Phishing
- Grayware

Viruses

Viruses are self-replicating code that install copies of themselves into other programs or data files for boot sectors of storage devices. Viruses can often carry a “payload” which performs some undesirable function. These functions can include but are not limited to:

- Stealing drive space
- Stealing CPU cycles
- Accessing private information
- Corrupting data
- Digital defacement or vandalism
- Spamming contact lists

Worms

A worm is a piece of standalone computer code that replicates itself in order to spread to other computers. It normally uses a computer network to spread itself, using security vulnerabilities on the target computer or network to propagate. Unlike a virus, it does not attach itself to an existing file. Even if there is no payload, worms consume resources such as bandwidth and storage space just through their act of replication.

Trojan horses

A Trojan horse, or Trojan is malware that is defined by its delivery method. Through the use of social engineering, or some other method, the code is installed on a system by a valid user of the system and like the original Trojan horse there is something more than advertised within the software. Trojans, unlike worms or viruses are generally non-self-replicating. The most common payload of a Trojan is the setting up of a “backdoor” control mechanism to the system that it is installed on.

Ransomware

Ransomware is a type of malware that, as the name implies, hold the system ransom until payment of some kind is made. It does this by restricting access to the legitimate owner of the system either by encrypting files or locking the system. Usually, a message of some kind is displayed with the demands. Upon payment a utility or key is sent to the user to unlock the system.

Scareware

Scareware comes in two main flavours; the first tries to convince the user that his computer is infected with some non-existent malware, scaring the user into purchasing the author’s virus removal utility. The utility is nonfunctional or some additional form of malware.

The second form tries to convince the user that the computer has been or is being used for an illegal act, such as being part of a botnet or storing child pornography. Again, the objective is to scare the user into paying to cure something that is not really there.

Spyware

Spyware is used by its authors to collect information about the user and its computer without the user's knowledge. The end result can be as benign as being better able to target ads, to as criminal as key loggers designed to record account ids and passwords of bank accounts and forward them off to the authors.

Adware

Adware is not malware per se. It is merely any software that produces advertisements in order to generate revenue for its author. While a lot of people find this inconvenient or irritating, it is not malware. As such, it is not blocked by the antivirus software for being malware.

Software that has adware built into it will be blocked if it has malware in it.

Botnets

A botnet is a network of Internet connected computers that have been covertly usurped to forward transmissions to other computers on the Internet on behalf of a “master”. These transmissions can be minimally damaging, such as spam, or they can critically impact a target as when used to launch a Distributed Denial of Service attack.

Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based.

According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

See also: Botnet protection.

Phishing

Phishing is a social engineering technique that is used to obtain sensitive and confidential information by masquerading as a communication from a trusted entity such as a well-known institution, company, or website. Usually, the malware is not in the communication itself but in the links within the communication.

Grayware

Grayware programs are unsolicited software programs installed on computers, often without the user’s consent or knowledge. Grayware programs are generally considered an annoyance, but they can also cause system performance problems or be used for malicious purposes.

AntiVirus scanning order

The antivirus scanning function includes various modules and engines that perform separate tasks.

FortiOS has two different modes of antivirus scanning: **proxy-based** and **flow-based**. The reasons for the different modes are performance and granularity. In just about everything relating to security there is a constant balancing act going on. As the level of security and comprehensiveness increases, there is by necessity a decrease in either convenience or performance or both. The increase in processing to scan for more threats requires more resources; resources that are a finite supply on the hardware. Granularity can sometimes be used to mitigate performance impact by scanning for a smaller subset of traffic but this is only recommended when that smaller subset of traffic is the only traffic going through the firewall.

If the traffic on the device is slight, then the impact on the performance will hardly be noticeable. But if the unit is working close to capacity in terms of traffic and there are a lot of files coming through, then there might be a noticeable decline in the performance.

While both modes offer significant security, proxy-based is weighted towards being more thorough and easily configurable, while flow-based is designed to optimize performance.

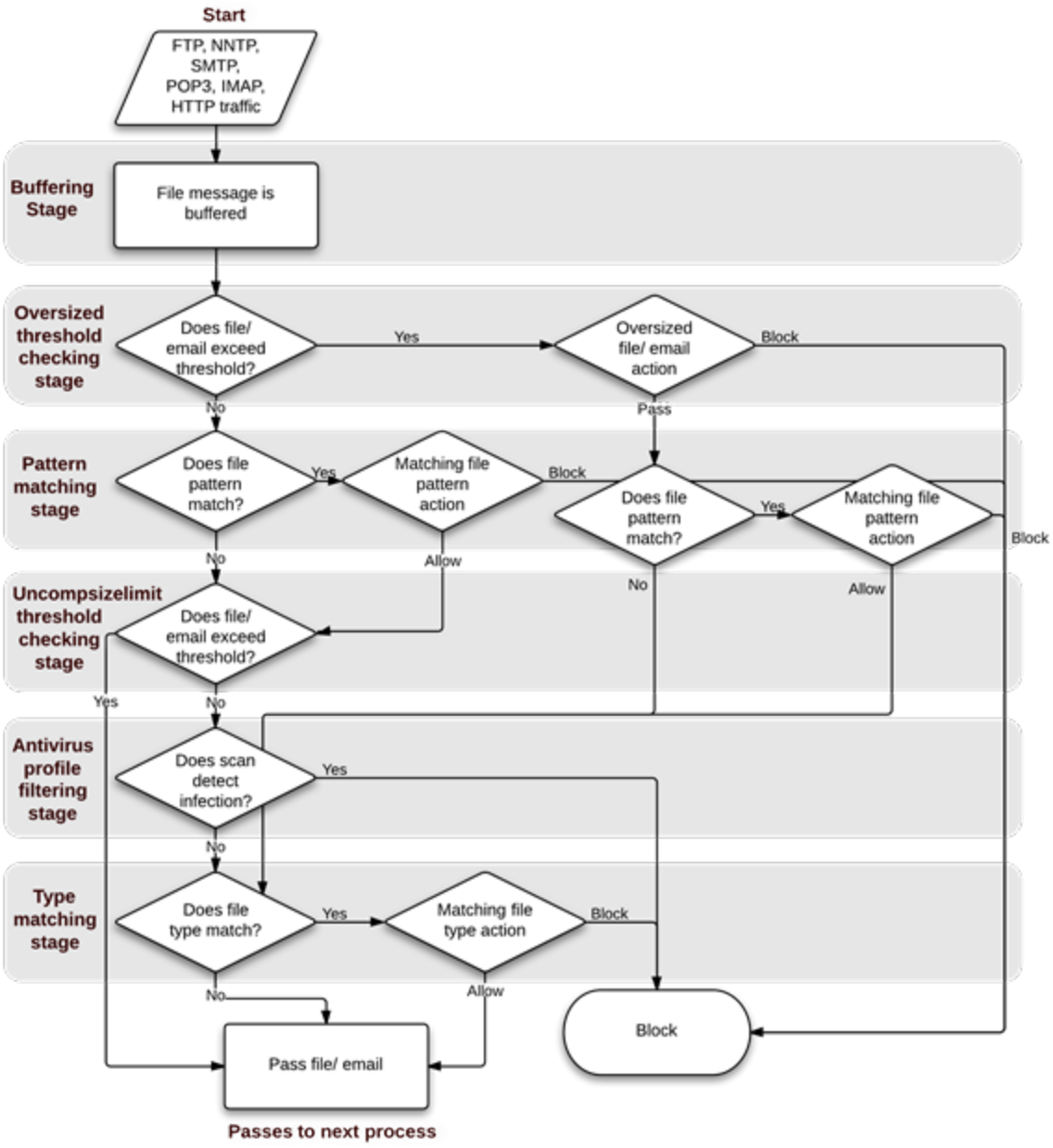
See Antivirus scanning differences in FortiOS 5.0, 5.2, 5.4, and 5.6 in the Inspection Modes section for more details on flow vs. proxy inspection modes on your FortiGate.

Proxy-based antivirus scanning order

The following figure illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The `uncompsizelimit` check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the `config antivirus service` command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics, if enabled.

File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.

Antivirus scanning order when using the normal, extended, or extreme database

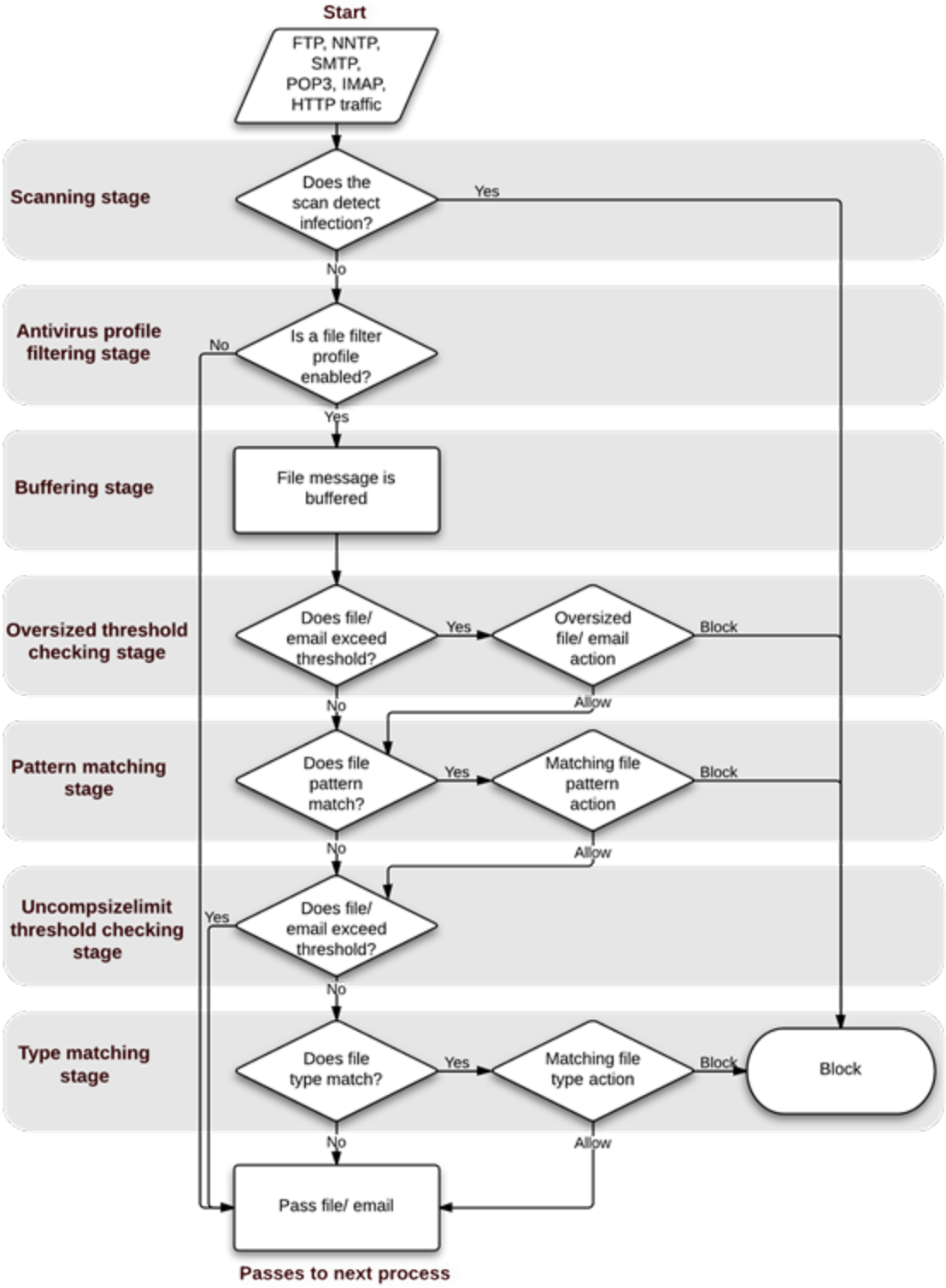


If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file `fakefile.EXE` is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.

Flow-based antivirus scanning order

The following figure illustrates the antivirus scanning order when using flow-based scanning (i.e. the flow-based database). The antivirus scan takes place before any other antivirus-related scan. If file filter is not enabled, the

file is not buffered. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.



AntiVirus databases

The antivirus scanning engine relies on a database of virus signatures to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.

All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.

Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.

If your FortiGate unit supports extended, extreme, or flow-based virus database definitions, you can select the virus database most suited to your needs.

If you require the most comprehensive antivirus protection, enable the extended virus database. The additional coverage comes at a cost, however, because the extra processing requires additional resources.

To change the antivirus database

Use the CLI to run the following commands:

```
config antivirus settings
   set default-db extended
end
```

AntiVirus techniques

The first three antivirus features in the list below work in sequence to efficiently scan incoming files and offer your network optimal antivirus protection. The first two features have specific functions, the third, heuristics, protects against new or previously unknown virus threats.

- **Virus scan**
  If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN).

- **Grayware protection**

  If the file passes the virus scan, it can be checked for grayware. Grayware scanning is an optional function and

must be enabled in the CLI if it is to be scanned for along with other malware. Grayware cannot be scanned for on its own. While done as a separate step, antivirus scanning must be enabled as well.

To enable grayware detection enter the following in the CLI:

```
config antivirus settings
   set grayware enable
end
```

To disable grayware detection enter the following in the CLI:

```
config antivirus settings
   set grayware disable
end
```

Grayware signatures are kept up to date in the same manner as the antivirus definitions.

- **Heuristics**

  After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.

  To set heuristics, enter the following in the CLI:

  ```
  config antivirus heuristic
     set mode {pass | block |disable}
  end
  ```

  - "`block`" enables heuristics and any files determined to be malware are blocked from entering the network.
  - "`pass`" enables heuristics but any files determined to be malware are still allowed to pass through to the recipient.
  - "`disable`" turns off heuristics.

- **FortiGuard AntiVirus**

  The FortiGuard Antivirus services are included in the regular FortiGuard subscription and include automatic updates of antivirus engines and definitions as well as a DNS black list (DNSBL) through the FortiGuard Distribution Network (FDN).

  Current information about your subscription and version numbers can be found at **System > FortiGuard.** This page will also allow the configuration of connections to the FortiGuard Center and how often to check for updates to the antivirus files.

Updating antivirus definitions can cause a short disruption of traffic being scanned while the FortiGate unit applies the new signature database. Schedule updates for time periods when traffic is light to minimize disruption.

- Botnet protection

  A botnet is a network of Internet connected computers that have been covertly usurped to forward transmissions to other computers on the Internet on behalf of a "master". These transmissions can be minimally damaging, such as spam, or they can critically impact a target as when used to launch a Distributed Denial of Service attack.

Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based.

The latest botnet database is available from FortiGuard. To see the version of the database and display its contents, go to **System > FortiGuard > AntiVirus >** and you will see data for **Botnet IPs** and **Botnet Domains**. You can also block, monitor, or allow outgoing connections to botnet sites for each FortiGate interface.

- **Quarantine / Source IP ban**

  As of FortiOS 5.2, quarantine was a place where traffic content was held in storage where it couldn't interact with the network or system. This was removed, but the term quarantine was kept to describe keeping selected source IPs from interacting with the network and protected systems. This source IP ban is kept in the kernel rather than in any specific application engine and can be queried by APIs. The features that can use the APIs to access and use the banned source IP addresses are antivirus, DLP, DoS and IPS. Both IPv4 and IPv6 version are included in this feature.

  You quarantine a source address through the GUI. Go to **FortiView > Sources**. Right-click on the source address you wish to quarantine and select **Quarantine Source Address**. You can set the duration of the quarantine in days, hours, minutes, or seconds. A User Quarantine ban can be removed in **Monitor > User Quarantine Monitor**.

  To configure the AntiVirus security profile to add the source IP address of an infected file to the quarantine or list of banned source IP addresses in the CLI:

```
config antivirus profile
   edit <name of profile>
      config nac-quar
         set infected quar-src-ip
         set expiry 5m
      end
```

  If the `quar-src-ip` action is used, the additional variable of expiry time will become available. This variable determines for how long the source IP adddress will be blocked. In the CLI the option is called `expiry` and the duration is in the format `<###d##h##m>`. The maximum days value is 364. The maximum hour value is 23 and the maximum minute value is 59. The default is 5 minutes.

FortiGuard AntiVirus updates

To ensure that your system receives the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard AntiVirus services. To configure this feature, go to **System > FortiGuard**. Under **AntiVirus & IPS Updates**, enable **Scheduled Updates**. From here you can schedule updates to occur on a consistent weekly, daily, or even hourly basis.

Updating antivirus definitions can cause a short disruption of traffic being scanned while the FortiGate unit applies the new signature database. Schedule updates for time periods when traffic is light to minimize disruption.

FortiSandbox

Not every piece of malware has a signature. This is especially true of new malware and variations on existing malware. FortiOS can upload suspicious files to FortiSandbox for sandbox inspection. When a FortiGate uses sandbox inspection, files are sent to the FortiSandbox. Then the FortiSandbox uses virtual machines (VMs) running different operating systems to test the file, to determine if it is malicious. If the file exhibits risky behavior, or is found to contain a virus, a new signature can be added to both the local FortiGate malware database and the FortiGuard AntiVirus signature database.

A file is deemed suspicious when it does not contain a known threat but has characteristics that suggest it may be malware. The characteristics that determine if a file is suspicious are updated by Fortinet to reflect the current threat climate.

FortiSandbox is available as a physical or virtual appliance (FortiSandbox Appliance), or as a cloud advanced threat protection service integrated with FortiGate (FortiCloud).

To configure an AntiVirus profile to send files to FortiSandbox, first verify that your FortiSandbox appliance is configured or that your FortiCloud account is active. Then go to **Security Profiles > AntiVirus** and enter the desired **Inspection Options**.

Sandbox inspection assists in the discovery of new threats and the creation of new signatures to be added to the global FortiGuard AntiVirus database. Files deemed malicious are immediately added to a custom Malware Package, which the FortiGate downloads every two minutes for live detection.

The **Advanced Threat Protection Statistics** dashboard widget displays the number of files that your FortiGate unit has uploaded or submitted to FortiSandbox. To see FortiSandbox statistics for the last 7 days, go to **Fortinet Security Fabric> Settings**.

Option for "Suspicious Files Only" for FortiSandbox submissions

Beginning in FortiOS 6.0.1, FortiGates can use the FortiSandbox Cloud service as part of the AntiVirus subscription. In order to reduce client upload bandwidth usage and general load on the FortiSandbox service, a new "Suspicious Files Only" upload option has been added to the AntiVirus profile, which previously only had "None" and "All Supported Files".

In order to enforce best practices, "None" is now the default.

Syntax

```
config antivirus profile
   edit <profile name>
      set ftgd-analytics [disable|suspicious|everything]
   end
```

Client comforting

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit scans it. If no infection is found, the file is sent along to the client. The client initiates the file transfer and nothing happens until the FortiGate finds the file clean, and releases it. Users can be impatient, and if the file is large or the download slow, they may cancel the download, not realizing that the transfer is in progress.

The client comforting feature solves this problem by allowing a trickle of data to flow to the client so they can see the file is being transferred. The default client comforting transfer rate sends one byte of data to the client every

ten seconds. This slow transfer continues while the FortiGate unit buffers the file and scans it. If the file is infection-free, it is released and the client will receive the remainder of the transfer at full speed. If the file is infected, the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file.

If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.

Client comforting can send unscanned and potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS and FTPS traffic.

Enable and configure client comforting

1. Go to **Security Profiles > Proxy Options**.
2. Select a Proxy Options profile and choose **Edit**, or select **Create New** to make a new one.
3. Scroll down to the **Common Options** section and enable the **Comfort Clients** feature. This will set the option on all of the applicable protocols. The ability to set this feature on a protocol by protocol basis exists in the CLI.
4. Select **OK** or **Apply** to save the changes.
5. Apply this Proxy Options profile in any security policy for it to take effect on all traffic handled by the policy.

The default values for Interval and Amount are 10 and 1, respectively. This means that when client comforting takes effect, 1 byte of the file is sent to the client every 10 seconds. You can change these values to vary the amount and frequency of the data transferred by client comforting.

Oversized files and emails

Downloaded files can range from a few Kilobytes to multiple Gigabytes. A FortiGate doesn't have the memory to allow for a large number of people downloading large files. Imagine the memory required for a team of developers to all download the latest Linux OS distribution at once, in addition to the normal requirements of the firewall. Everything would come to a grinding halt if the FortiGate tried to store each of those Gigabyte+ files in memory. To give you some piece of mind, the chances of malware being in a large file like those is much smaller than in a smaller single Megabyte file, so the threat is somewhat limited, but you will probably want to use your computers antivirus software to scan those large files after they have been downloaded.

A threshold must be set to prevent the resources of the system from becoming overloaded. By default the threshold is 10 MB. Any files larger than the threshold will not be scanned for malware. With a maximum file size threshold in place, it must now be determined what is to be done with the files that are larger than threshold. There are only 2 choices; either the file is passed through without being scanned for malware or the file is blocked. The default action for oversized files is to pass them through.

If you wish to block the downloading of files over the threshold, this can be set within the Proxy Option profile found at **Security Profiles > Proxy Options**, under **Common Options**.

Enable **Block Oversized File/Email**.

This will reveal an additional option, **Threshold (MB)**. The threshold of the files is set based upon the protocol being used to transfer the file. In the CLI and configuration file, the threshold variable is found in each of the protocol sections within the profile. Changing the value in this field will change the `oversize-limit` value for all of the protocols.

If you wish to change the `oversize-limit` value on the protocols covered in a Proxy Option profile you have two options.

1. You can go into the CLI and change the value manually within each of the protocol sections.
2. You can use the GUI to temporarily block oversized files, and when configuring it change the threshold to the new value that you want. Apply this setting. Then go back to the profile and turn off the block setting. If you now go into the CLI you will find that the configuration file has retained the new oversize-limit value.

The settings can be found in the CLI by going to:

```
config firewall profile-protocol-options
   edit <profile_name>
      config <protocol>
         set oversize-limit <size_int>
      end
   end
end
```

Archive scan depth

The antivirus scanner will open archives and scan the files inside. Archives within other archives, or nested archives, are also scanned to a default depth of twelve nestings. You can adjust the number of nested archives the FortiGate unit will scan with the `uncompressed-nest-limit` CLI command. Further, the limit is configured separately for each traffic type.

Configuring archive scan depth

For example, this CLI command sets the archive scan depth for SMTP traffic to 5. That is, archives within archives will be scanned five levels deep.

```
config firewall profile-protocol-options
   edit "default"
      config http
         set uncompressed-nest-limit 5
      end
   end
end
```

You can set the nesting limit from 2 to 100.

Scan buffer size

When checking files for viruses, there is a maximum file size that can be buffered. Files larger than this size are passed without scanning. The default size for all FortiGate models is 10 megabytes.

Archived files are extracted and email attachments are decoded before the FortiGate unit determines if they can fit in the scan buffer. For example, a 7 megabyte ZIP file containing a 12 megabyte EXE file will be passed without scanning with the default buffer size. Although the archive would fit within the buffer, the uncompressed file size will not.

Configuring the uncompression buffer

In this example, the `uncompressed-oversize-limit` CLI command is used to change the scan buffer size to 20 megabytes for files found in HTTP traffic:

```
config firewall profile-protocol-options
   edit <profile_name>
      config http
         set uncompressed-oversize-limit 20
      end
   end
end
```

The maximum buffer size varies by model. Enter `set uncompressed-oversize-limit ?` to display the buffer size range for your FortiGate unit.

Windows file sharing (CIFS)

FortiOS supports virus scanning of Windows file sharing traffic. This includes CIFS, SMB, and SAMBA traffic. This feature is applied by enabling SMB scanning in an antivirus profile and then adding this profile to a security policy that accepts CIFS traffic. CIFS virus scanning is available only through flow-based antivirus scanning.

FortiOS flow-based virus scanning can detect the same number of viruses in CIFS/SMB/SAMBA traffic as it can for all supported content protocols.

Note the following about CIFS/SMB/SAMBA virus scanning:

- Some newer version of SAMBA clients and SMB2 can spread one file across multiple sessions, preventing some viruses from being detected if this occurs.
- Enabling CIFS/SMB/SAMBA virus scanning can affect FortiGate performance.
- SMB2 is a new version of SMB that was first partially implemented in Windows Vista.
- Currently SMB2 is supported by Windows Vista or later, and partly supported by Samba 3.5 and fully support by Samba 3.6.
- The latest version of SMB2.2 will be introduced with Windows 8.
- Most clients still use SMB as default setting.

Configuring CIFS/SMB/SAMBA virus scanning

Use the following command to enable CIFS/SMB/SAMBA virus scanning in an antivirus profile:

```
config antivirus profile
   edit <smb-profile>
      config smb
         set options scan
      end
```

Then add this antivirus profile to a security policy that accepts the traffic to be virus scanned. In the security policy the service can be set to ALL, SAMBA, or SMB.

```
config firewall policy
   edit <policy-id-integer>
      set service ALL
      ...
      set utm-status enable
      set av-profile <smb-profile>
   end
```

Enabling AntiVirus scanning

Antivirus scanning is configured in an AntiVirus profile, but it is enabled in a firewall policy. Once the use of an AntiVirus profile is enabled and selected in one or more firewall policies, all the traffic controlled by those firewall policies will be scanned according to the settings in that profile.

By going to **System > Feature Visibility,** you can enable or disable two aspects of the AntiVirus Profile.

1. **AntiVirus** will determine if the option to use AntiVirus profiles is available.
2. **Multiple Security Profiles** will determine if you can configure any AntiVirus profiles beyond the default profile.

The use of antivirus protection is a minimum standard for security protection. The question left to decide is whether or not you wish to use multiple profiles in your configuration.

From **Security Profiles > AntiVirus** you can edit existing profiles or create and configure new antivirus profiles that can then be applied to firewall policies. A profile is specific configuration information that defines how the traffic within a firewall policy is examined and what action may be taken based on the examination.

The configuration of the antivirus profile depends on whether the inspection mode is proxy-based or flow-based. You select the inspection mode by going to the **System > Settings** page. The FortiGate's inspection mode is also displayed on the unit's **Dashboard** in the **System Information** widget.

The discussion of the differences in antivirus scanning modes helps to understand how this scanning works in proxy- and flow-based inspection, as well as in different versions of FortiOS 5.x.

Enabling AntiVirus in Proxy-mode - GUI

1. Go to **Security Profiles > AntiVirus**.
2. Choose whether you want to edit an existing profile or create a new one.
   - The default profile will be the one displayed by default.
   - If you are going to edit an existing profile, selecting it can be done by either using the drop down menu in the upper right hand corner of the window or by selecting the List icon (the furthest right of the 3 icons in the upper right of the window, if resembles a page with some lines on it), and then selecting the profile you want to edit from the list.
   - If you need to create a new profile you can either select the **Create New** icon (a plus sign within a circle) or select the **List icon** and then select the **Create New** link in the upper left of the window that appears.
3. If you are creating a new profile, write a name for it in the **Name** field.
4. For the **Detect Viruses** field, select either **Block** to prevent infected files from passing throughout the FortiGate or **Monitor** to allow infected files to pass through the FortiGate but to record instances of infection.
5. Under **Inspected Protocols**, enable the protocols you wish to be blocked or monitored.
6. Under **APT Protection Options**, you may enable the following: **Content Disarm and Reconstruction**, **Treat Windows Executables in Email Attachments as Viruses** and **Send Files to FortiSandbox Cloud for Inspection**, and **Use Virus Outbreak Prevention Database**.

   FortiSandbox options are only available if you have a FortiCloud account active on your FortiGate.
7. Select **Apply**.
8. Add the AntiVirus profile to a firewall security policy.

To view Mobile Malware license and version information, go to **System > FortiGuard** and locate the Mobile Malware section in the **License Information** table.

Content Disarm and Reconstruction (CDR)

Content Disarm and Reconstruction (CDR) is used to remove exploitable content and replace it with content that is known to be safe. As the files are processed through an enabled Proxy-based AntiVirus profile, content that is deemed malicious or unsafe is replaced with content that will allow the traffic to continue, but not put the recipient at risk.

Content that can be scanned includes PDF and Microsoft Office files leaving the network on CDR-supported protocols (HTTP web download, SMTP email send, IMAP/POP3 email retrieval—MAPI is not supported).

This feature will work without FortiSandbox configured, but only if you wish to discard the original file. If FortiSandbox is configured and it responds that the file is clean, it will pass the content unmodified.

This feature will not work if `splice` or `client-comfort` are enabled under `profile-protocol-options` for SMTP.

CDR does not alter documents in an HTTP POST, and is not designed to strip content leaving the network for HTTP. It only works on HTTP GET.

Syntax

The use of CDR is enabled or disabled separately for each protocol in the profile. Note that all CDR commands are only available when you set the profile's `inspection-mode` to `proxy`.

```
config antivirus profile
   edit <name>
      set inspection-mode proxy
      config <protocol>
         set options scan
         set content-disarm {enable | disable}
      next
   end
end
```

You must ensure that `set options scan` is configured.

If `set options av-monitor` is configured for a protocol, it will enable the `detect-only` option (see below) and CDR will not occur for that protocol.

The enabling and disabling of the CDR is specific to the protocol, but the granular configuration of which types of content will be rewritten by the CDR engine are configured based on the AntiVirus profile. The settings within the `config content-disarm` context are applicable to all of the CDR enabled protocols.

```
config antivirus profile
   edit <name>
      config content-disarm
         set original-file-destination {fortisandbox | quarantine | discard}
         set office-macro {enable | disable}
         set office-hylink {enable | disable}
         set office-linked {enable | disable}
         set office-embed {enable | disable}
         set pdf-javacode {enable | disable}
         set pdf-embedfile {enable | disable}
         set pdf-act-gotor {enable | disable}
         set pdf-act-launch {enable | disable}
```

```
            set pdf-act-uri {enable | disable}
            set pdf-act-sound {enable | disable}
            set pdf-act-movie {enable | disable}
            set pdf-act-java {enable | disable}
            set pdf-act-form {enable | disable}
            set cover-page {enable | disable}
            set detect-only {enable | disable}
        next
    end
end
```

Where:

Option	Description
`original-file-destination`	Select the destination to which files will be sent for inspection. Note that, once you enable `content-disarm` under a protocol, you will be warned that all original files will be discarded. To be able to retrieve the original files, you must set an `original-file-destination` for this profile.
`office-macro`	Enables/disables stripping of macros in Microsoft Office documents.
`office-hylink`	Enables/disables stripping of hyperlinks in Microsoft Office documents.
`office-linked`	Enables/disables stripping of linked objects in Microsoft Office documents.
`office-embed`	Enables/disables stripping of embedded objects in Microsoft Office documents.
`pdf-javacode`	Enables/disables stripping of JavaScript code in PDF documents.
`pdf-embedfile`	Enables/disables stripping of embedded files in PDF documents.
`pdf-act-gotor`	Enables/disables stripping of links to other PDFs in PDF documents.
`pdf-act-launch`	Enables/disables stripping of links to external applications in PDF documents.
`pdf-act-uri`	Enables/disables stripping of links to URI resources in PDF documents.
`pdf-act-sound`	Enables/disables stripping of embeded sound files in PDF documents.
`pdf-act-movie`	Enables/disables stripping of embeded movies in PDF documents.
`pdf-act-java`	Enables/disables stripping of actions that execute JavaScript code in PDF documents.
`pdf-act-form`	Enables/disables stripping of actions that submit data to other targets in PDF documents.
`cover-page`	Enables/disables inserting a cover page into the disarmed document.
`detect-only`	Enables/disables only detect disarmable files, do not alter content.

When the antivirus profile successfully detects suspicious content and strips the data, a new page is appended to the start of the document with a message that reads "*This file has been cleaned of potential threats*".

You can `set cover-page disable` (see above) if you do not want a cover page appended to any disarmed content.

FortiGuard virus outbreak prevention

FortiGuard virus outbreak prevention uses checksums to filter files in order to detect and prevent quick virus outbreaks, because it usually takes at least a few hours for FortiGuard to develop and push signatures and a virus outbreak can do a lot of damage within that time period. This method proves to be quite effective using hash values of probable virus files.

Enable this feature under **Security Profiles > AntiVirus > Use Virus Outbreak Prevention Database**. Note that this feature requires a license, which you can obtain through **System > FortiGuard > Outbreak Prevention**.

Syntax

Note that `outbreak-prevention` is only available when `options` is set to `scan`:

```
config antivirus profile
   edit <name>
      config <protocol>
         set options scan
         set outbreak-prevention {disabled | files | full-archive}
      next
   ...
```

where `full-archive` analyzes files including the contents of archives, as opposed to `files` which does not include the contents of archives.

Enabling AntiVirus in Flow-mode - GUI

1. Go to **Security Profiles > AntiVirus**.
2. Choose whether you want to edit an existing profile or create a new one.
   - The default profile will be the one displayed by default.
   - If you are going to edit an existing profile, selecting it can be done by either using the drop down menu in the upper right hand corner of the window or by selecting the List icon (the furthest right of the 3 icons in the upper right of the window, if resembles a page with some lines on it), and then selecting the profile you want to edit from the list.
   - If you need to create a new profile you can either select the **Create New** icon (a plus sign within a circle) or select the **List icon** and then select the **Create New** link in the upper left of the window that appears.
3. If you are creating a new profile, write a name for it in the **Name** field.
4. Select **Quick** or **Full Scan Mode**(see the discussion of the differences in antivirus scanning modes for more information).
5. For the **Detect Viruses** field, select either **Block** to prevent infected files from passing throughout the FortiGate or **Monitor** to allow infected files to pass through the FortiGate but to record instances of infection.
6. Under **Inspected Protocols**, enable the protocols you wish to be blocked or monitored.
7. Under **Inspection Options**, you may enable the following: **Treat Windows Executables in Email Attachments as Viruses** and **Include Mobile Malware Protection**.

You may also enable the following options if you have a FortiCloud account active on your FortiGate: **Send Files to FortiSandbox Cloud for Inspection** and **Use FortiSandbox Database**.

8. Select **OK** or **Apply**.
9. Add the AntiVirus profile to a firewall security policy.

Enabling AntiVirus - CLI

Configure the scan option for each type of traffic you want scanned.

1. Configure the AntiVirus profile

```
config antivirus profile
   edit <profile_name>
      set comment "scan and delete virus"
      set replacemsg-group ''
      set scan-botnet-connections block
      set ftgd-analytics suspicious
      config http
         set options scan
      end
      config ftp
         set options scan
      end
      config imap
         set options scan
      end
      config pop3
         set options scan
      end
      config smtp
         set options scan
      end
      config nntp
         set options scan
      end
      config smb
         set options scan
      end
   end
```

2. Add the AntiVirus profile to the Fortigate firewall security policy. When using the CLI, you will need to know the policy ID number.

```
config firewall policy
   edit <policy ID number>
      set av-profile <profile_name>
      set profile-protocol-options default
   end
end
```

Overriding the AV engine file scan timeout

Overriding the AV engine file scan timeout allows the FortiGate to scan files as large as 4GB without breaking the scan.

Override the large file scan timeout value in seconds (30 - 3600). Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.

Syntax

```
config antivirus settings
   set override-timeout 0
end
```

Testing your antivirus configuration

You have configured your FortiGate unit to stop viruses, but you'd like to confirm your settings are correct. Even if you have a real virus, it would be dangerous to use for this purpose. An incorrect configuration will allow the virus to infect your network.

To solve this problem, the European Institute of Computer Anti-virus Research has developed a test file that allows you to test your antivirus configuration. The EICAR test file is not a virus. It cannot infect computers, nor can it spread or cause any damage. It's a very small file that contains a sequence of characters. Your FortiGate unit recognizes the EICAR test file as a virus so you can safely test your FortiGate unit antivirus configuration.

Go to http://www.fortiguard.com/antivirus/eicartest.html to download the test file (eicar.com) or the test file in a ZIP archive (eicar.zip).

If the antivirus profile applied to the security policy that allows you access to the Web is configured to scan HTTP traffic for viruses, any attempt to download the test file will be blocked. This indicates that you are protected.

Example scenarios

The following examples provide sample antivirus configuration scenarios.

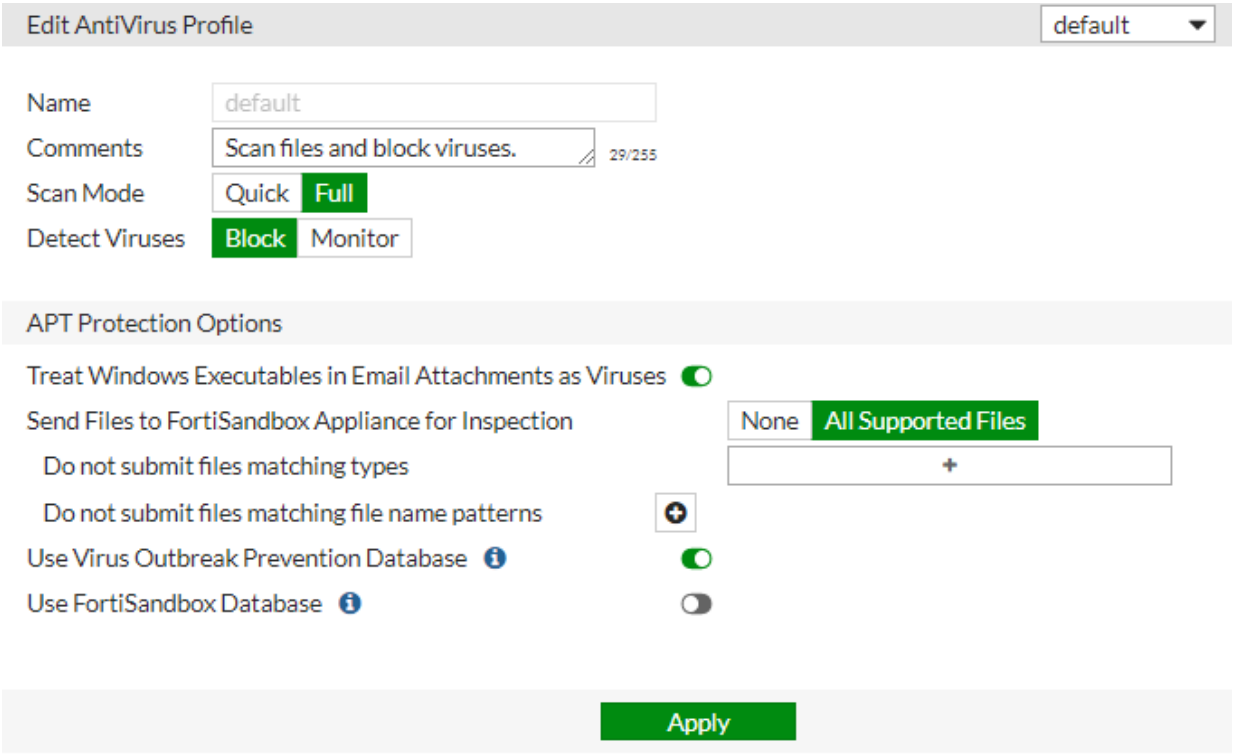
Configuring simple default AntiVirus profile

If performance is not a real concern and the FortiGate's resources are not being stretched, it is perfectly reasonable to create one AntiVirus profile that covers the range of uses found in your environment. This example is one possible default configuration.

Context:

- This is an edited default profile and will be used on all security policies
- It will need to scan for malware on all available protocols.
- Malware, botnets, and grayware should be blocked
- The inspection method should be flow-based
- A current FortiCloud account is available

Creating the profile - GUI



1. In the following fields, enter the settings shown in the screenshot.
2. Select **Apply**.
3. Enable grayware scanning through the CLI.

```
config antivirus settings
   set grayware enable
end
```

Creating the profile - CLI

1. Enter the CLI by one of the following methods:
   - SSH through a terminal emulator
   - CLI Console access
   - FortiExplorer's CLI mode
2. Enter the following commands:

```
config antivirus profile
   edit default
      set comment "scan and delete virus"
      set inspection-mode flow-based
      set scan-botnet-connections block
      set ftgd-analytics suspicious
      config http
         set options scan
         end
      config ftp
         set options scan
         end
```

```
        config imap
           set options scan
           end
        config pop3
           set options scan
           end
        config smtp
           set options scan
           end
        config nntp
           set options scan
           end
        config smb
           set options scan
           end
end
```

3. Enable grayware scanning

```
   config antivirus settings
      set grayware enable
      end
```

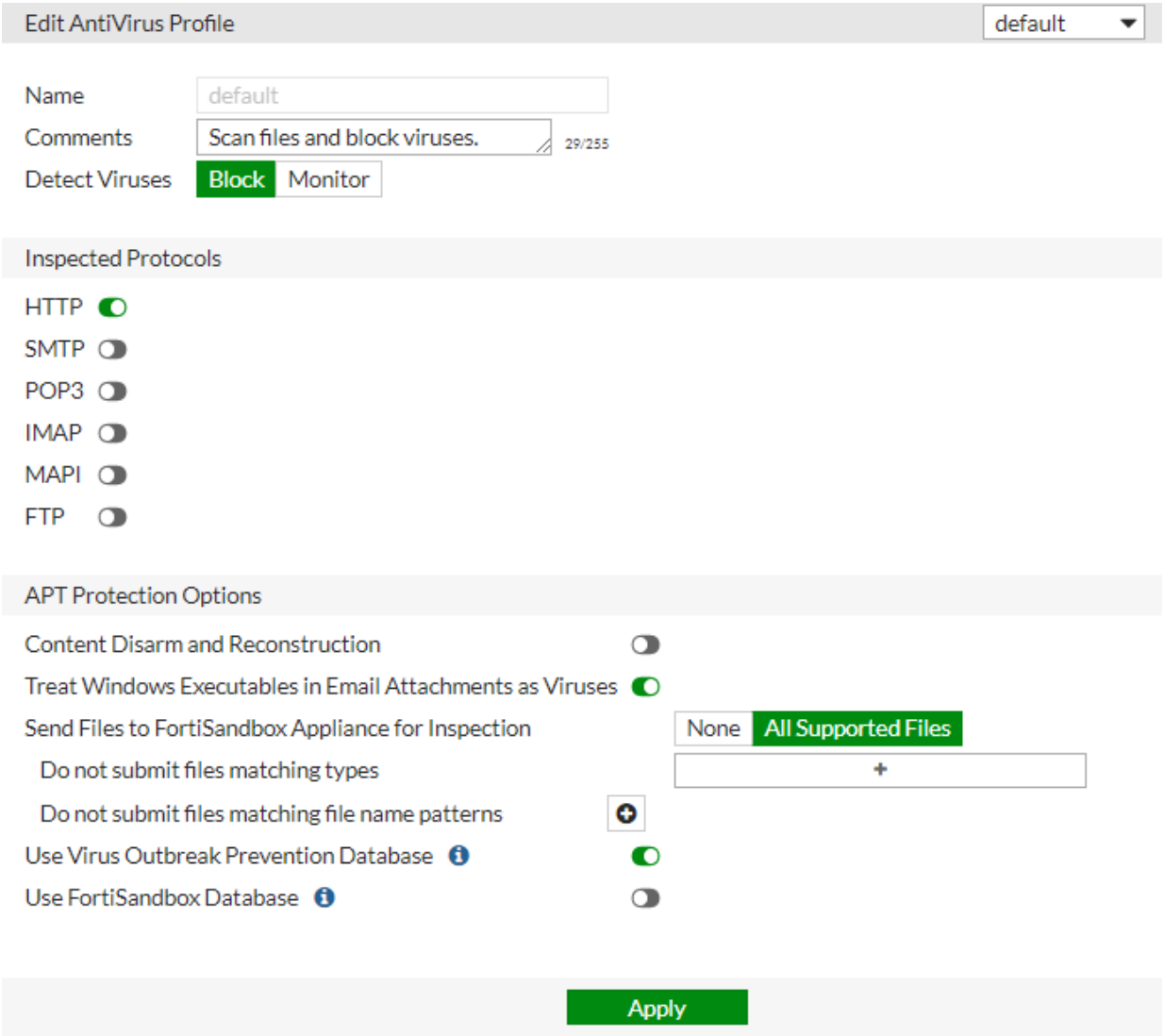
Setting up a basic proxy-based AntiVirus profile for email traffic

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable antivirus protection on a FortiGate unit located in a satellite office.

Context:

- The satellite office does not have an internal email server. To send and retrieve email, the employees connect to an external mail server.
- There is a specific firewall security profile that handles the email traffic from the Internet to the mail server. The only traffic on this policy will be POP3 and IMAP and SMTP
- The company policy is to block viruses and connections to botnets.
- The FortiGate unit is a small model and the Internet bandwidth is limited so the policy is to not submit files to the FortiSandbox.

Creating the profile - GUI



1. In the following fields, enter the settings shown below:

Name	email-av
Comments	Scans email traffic from Internet for malware
Detect Viruses	Block
Inspected Protocols	all checked (HTTP, SMTP, POP3, IMAP, MAPI, and FTP).
Content Disarm and Reconstruction	checked (optional) - used to remove exploitable content and replace it with content that is known to be safe. For more information, see Content Disarm and Reconstruction (CDR)

Original File Destination	Destination to which files will be sent for inspection: FortiSandbox, File Quarantine, or Discard.
Treat Windows Executables in Email Attachments as Viruses	checked - also optionally decide whether or not to submit files matching particular types and/or file name patterns.
Send Files to FortiSandbox Appliance for Inspection	checked (All Supported Files).
Use Virus Outbreak Prevention Database	checked - used to preempt outbreaks before AV Signatures are created.
Use FortiSandbox Database	checked - supplements the AV Signature database.

2. Select **Apply**.

Creating the profile - CLI

1. Enter the CLI by one of the following methods:
   - SSH through a terminal emulator
   - CLI Console widget
   - FortiExplorer's CLI mode
2. Enter the following commands:

```
config antivirus profile
   edit "email-av"
      set comment "Scans email traffic from Internet for malware"
      set inspection-mode proxy
      config content-disarm
         set original-file-destination {fortisandbox | quarantine | discard}
         set ...
      config <protocol>
         set options scan
         end
end
```

3. Additionally, if you wish to only send those files to FortiSandbox that heuristics determines as suspicious, enter the following (only available via the CLI):

```
config antivirus profile
   edit "email-av"
      set ftgd-analytics suspicious
end
```

For more information on how to strip content from various content types from documents (hyperlinks, linked objects, embedded objects, JavaScript code), see Content Disarm and Reconstruction (CDR) and the FortiOS 6.0 CLI Reference.

Adding the profile to a policy

In this scenario the following assumptions will be made:

- The policy that the profile is going to be added to is an IPv4 policy.
- The ID number of the policy is 11.

- The AntiVirus profile being added will be the "default" profile
- The SSL/SSH Inspection profile used will be the "default" profile

FortiClient enforcement has been moved from the Policy page to **Network > Interfaces** to enforce FortiClient registration on a desired LAN interface rather than a policy.

Adding the profile - GUI

1. Go to **Policy & Objects > IPv4 Policy**.
2. Use your preferred method of finding a policy.
   - If the ID column is available you can use that.
   - You can also choose based on your knowledge of the parameters of the policy
   - Select the policy with ID value of 11
3. In the Edit Policy window, go to the Security Profiles section
4. Turn ON AntiVirus, and in the drop down menu for the field, select default
5. If the AntiVirus profile is proxy-based the Proxy Options field and drop down menu will be revealed.
6. The SSL/SSH Inspection field will automatically be set to ON and one of the profiles will need to be selected from the drop down menu. In this case default is selected.
7. The log options will depend on your requirements and resources but to verify that everything is working properly, it is a good idea to turn ON logging of All Sessions after setting up a new profile and after giving some time for logs to accumulate
8. Turn on Antivirus.
9. Select an antivirus profile.
10. Select **OK** to save the security policy.

Adding the profile - CLI

To select the antivirus profile in a security policy — CLI

```
config firewall policy
   edit 11
      set utm-status enable
      set profile-protocol-options default
      set av-profile basic_antivirus
   end
```

Block files larger than 8 MB

Set proxy options profile to block files larger than 8 MB

1. Go to **Security Profiles > Proxy Options**.
2. Edit the default or select Create New to add a new one.
3. Scroll down to the common Options Section and place a check in the box next to BlockOversized File/Email
4. The sub line Threshold (MB) will appear with a value field. Enter 8.
5. Select **OK** or **Apply**.

The proxy options profile is configured, but to block files, you must select it in the firewall policies handling the traffic that contains the files you want blocked.

To select the Proxy Options profile in a security policy

1. Go to **Policy & Objects > IPv4 Policy** (or **IPv6 Policy**, depending).
2. Edit or create a security policy.
3. Select a proxy-based security profile. You will know that there is a proxy component to the Security Profile because when a Security Profile is Proxy based the Proxy Options field will be visible (for example, select an Antivirus profile that includes proxy scanning).
4. Beside Proxy Options select the name of the MTU proxy options protocol.
5. Select **OK** to save the security policy.
6. Once you complete these steps, any files in the traffic subject to Security Profile scanning handled by this policy that are larger than 8MB will be blocked. If you have multiple firewall policies, examine each to determine if you want to apply similar file blocking the them as well.

Web filter

This section describes FortiGate web filtering for HTTP traffic. The three main parts of the web filtering function, the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service interact with each other to provide maximum control over what users on your network can view as well as protection to your network from many Internet content threats. Web Content Filter blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic.

This Handbook chapter includes Inside FortiOS: Web Filtering and provides readers an overview of the features and benefits of key FortiOS components.

For further detail than the Inside FortiOS document, we provide the following topics:

Web filter concepts

Web filtering is a means of controlling the content that an Internet user is able to view. With the popularity of web applications, the need to monitor and control web access is becoming a key component of secure content management systems that employ antivirus, web filtering, and messaging security. Important reasons for controlling web content include:

- lost productivity because employees are accessing the web for non-business reasons
- network congestion — when valuable bandwidth is used for non-business purposes, legitimate business applications suffer
- loss or exposure of confidential information through chat sites, non-approved email systems, instant messaging, and peer-to-peer file sharing
- increased exposure to web-based threats as employees surf non-business-related web sites
- legal liability when employees access/download inappropriate and offensive material
- copyright infringement caused by employees downloading and/or distributing copyrighted material.

As the number and severity of threats increase on the World Wide Web, the risk potential increases within a company's network as well. Casual non-business related web surfing has caused many businesses countless hours of legal litigation as hostile environments have been created by employees who download and view offensive content. Web-based attacks and threats are also becoming increasingly sophisticated. Threats and web-based applications that cause additional problems for corporations include:

- spyware/grayware
- phishing
- pharming
- instant messaging
- peer-to-peer file sharing
- streaming media
- blended network attacks.

Spyware, also known as grayware, is a type of computer program that attaches itself to a user's operating system. It does this without the user's consent or knowledge. It usually ends up on a computer because of something the user does such as clicking on a button in a pop-up window. Spyware can track the user's Internet usage, cause unwanted pop-up windows, and even direct the user to a host web site. For further information, visit the FortiGuard Center.

Some of the most common types of grayware infection occur when:

- downloading shareware, freeware, or other forms of file-sharing services
- clicking on pop-up advertising
- visiting legitimate web sites infected with grayware.

Phishing is the term used to describe attacks that use web technology to trick users into revealing personal or financial information. Phishing attacks use web sites and email that claim to be from legitimate financial institutions to trick the viewer into believing that they are legitimate. Although phishing is initiated by spam email, getting the user to access the attacker's web site is always the next step.

Pharming is a next generation threat that is designed to identify and extract financial, and other key pieces of information for identity theft. Pharming is much more dangerous than phishing because it is designed to be completely hidden from the end user. Unlike phishing attacks that send out spam email requiring the user to click to a fraudulent URL, pharming attacks require no action from the user outside of their regular web surfing activities. Pharming attacks succeed by redirecting users from legitimate web sites to similar fraudulent web sites that have been created to look and feel like the authentic web site.

Instant messaging presents a number of problems. Instant messaging can be used to infect computers with spyware and viruses. Phishing attacks can be made using instant messaging. There is also a danger that employees may use instant messaging to release sensitive information to an outsider.

Peer-to-peer (P2P) networks are used for file sharing. Such files may contain viruses. Peer-to-peer applications take up valuable network resources and may lower employee productivity but also have legal implications with the downloading of copyrighted or sensitive company material.

Streaming media is a method of delivering multimedia, usually in the form of audio or video to Internet users. Viewing streaming media impacts legitimate business by using valuable bandwidth.

Blended network threats are rising and the sophistication of network threats is increasing with each new attack. Attackers learn from each successful attack and enhance and update their attack code to become more dangerous and to spread faster. Blended attacks use a combination of methods to spread and cause damage. Using virus or network worm techniques combined with known system vulnerabilities, blended threats can quickly

spread through email, web sites, and Trojan applications. Examples of blended threats include Nimda, Code Red, Slammer, and Blaster. Blended attacks can be designed to perform different types of attacks, which include disrupting network services, destroying or stealing information, and installing stealthy backdoor applications to grant remote access.

Different ways of controlling access

The methods available for monitoring and controlling Internet access range from manual and educational methods to fully automated systems designed to scan, inspect, rate and control web activity.

Common web access control mechanisms include:

- establishing and implementing a well-written usage policy in the organization on proper Internet, email, and computer conduct
- installing monitoring tools that record and report on Internet usage
- implementing policy-based tools that capture, rate, and block URLs.

The following information shows how the filters interact and how to use them to your advantage.

Order of web filtering

The FortiGate unit applies web filters in a specific order:

1. URL filter
2. FortiGuard Web Filter
3. web content filter
4. web script filter
5. antivirus scanning.

If you have blocked a FortiGuard Web Filter category but want certain users to have access to URLs within that pattern, you can use the **Override** within the FortiGuard Web Filter. This will allow you to specify which users have access to which blocked URLs and how long they have that access. For example, if you want a user to be able to access www.example.com for one hour, you can use the override to set up the exemption. Any user listed in an override must fill out an online authentication form that is presented when they try to access a blocked URL before the FortiGate unit will grant access to it.

If you have blocked a FortiGuard Web Filter category but want users within a specific Web Filter profile to have access to URLs within that pattern, you can use the following CLI command below to override (this will have no timeout affiliated to it):

CLI syntax:

```
config webfilter profile
   edit <profile>
      config web
      set whitelist exempt-av exempt-dlp exempt-rangeblock extended-log-others
      end
end
```

This command will set a Web Filter profile that exempts AV, DLP, RangeBlock, and supports extended log by FortiGuard whitelist.

Inspection modes

This topic briefly discusses proxy and flow-based inspection modes. For more information on flow vs. proxy inspection modes on your FortiGate and how they impact web filtering, see Individual Security Profile considerations in the Inspection Modes section.

Proxy

Proxy-based inspection involves buffering traffic and examining it as a whole before determining an action. The process of having the whole of the data to analyze allows for the examination of more points of data than the flow-based or DNS methods.

The advantage of a proxy-based method is that the inspection can be more thorough than the other methods, yielding fewer false positive or negative results in the data analysis.

Flow-based

The flow-based inspection method examines the file as it passes through the FortiGate unit without any buffering. As each packet of the traffic arrives it is processed and forwarded without waiting for the complete file or web page.

The advantage of the flow-based method is that the user sees a faster response time for HTTP requests and there is less chance of a time-out error due to the server at the other end responding slowly.

The disadvantages of this method are: (1) there is a higher probability of a false positive or negative in the analysis of the data; and, (2) a number of security features that can be used in the proxy-based method are not available in the flow-based inspection method. There are also fewer actions available based on the categorization of the website by FortiGuard services.

In flow mode, Web Filter profiles only include flow-mode features. Web filtering is still done with the same engines and to the same accuracy, but some inspection options are limited or not available in flow mode.

Configuring Web Filter profiles in flow-mode is different depending on the NGFW mode selected.

See "What's new in FortiOS 6.0.1" on page 15 and Individual Security Profile Considerations in the Inspection Modes section for more details on flow vs. proxy inspection modes on your FortiGate.

FortiGuard Web Filtering Service

FortiGuard Web Filtering is a managed web filtering solution available by subscription from Fortinet. Before you begin to use the FortiGuard Web Filtering options, verify that you have a valid subscription to the service for your FortiGate firewall.

FortiGuard Web Filtering enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest

FortiGuard Web Filtering Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface. FortiGuard Web Filtering supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).

FortiGuard Web Filtering includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filtering ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filtering Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.

FortiGuard web filtering and your FortiGate unit

When FortiGuard Web Filtering is enabled in a web filter or a DNS filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the FortiGate unit provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

FortiGuard web filtering actions

The possible actions are:

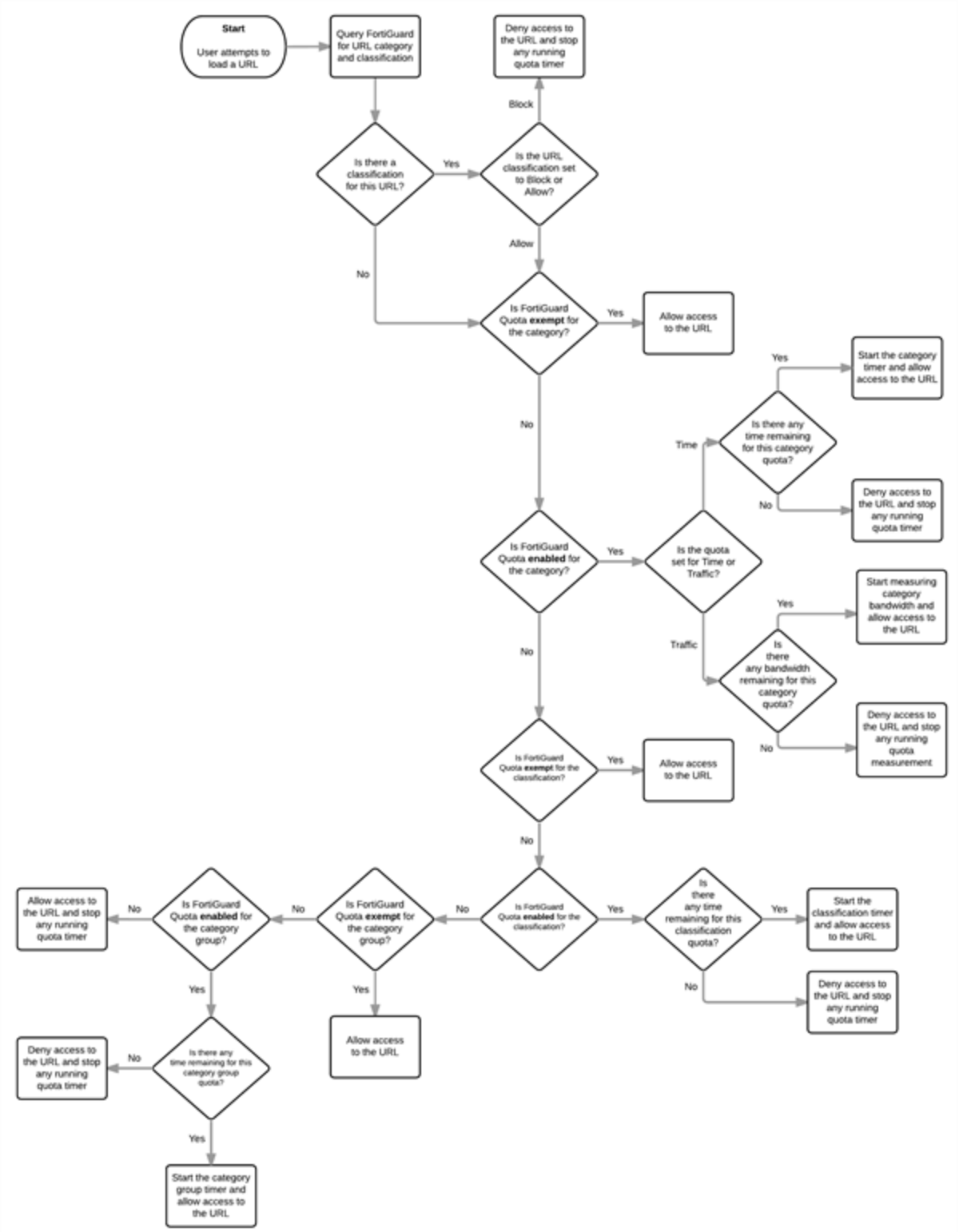
- **Allow** permits access to the sites within the category.
- **Block** prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
- **Monitor** permits and logs access to sites in the category. You may also enable user quotas when enabling the monitor action.
- **Warning** presents the user with a message, allowing them to continue if they choose.
- **Authenticate** requires a user to authenticate with the FortiGate unit before being allowed access to the category or category group.

The options of actions available will depend on the mode of inspection.

- Proxy - Allow, Block, Monitor, Warning, Authenticate and Disable.
- Flow-based, policy-based - Allow, Block & Monitor.
- Flow-based, profile-based - Allow, Deny

Configuring Web Filter profiles in flow-mode is different depending on the NGFW mode selected.

Web filtering flowchart



FortiGuard web filtering categories

The following tables identify each FortiGuard web filtering category (organized by group) along with associated category IDs. You can access the current list of category IDs through the CLI.

```
config webfilter profile
   edit default
      config ftgd-wf
         config filters
            edit 1
               set category ?
```

For a complete description of each web filtering category, visit http://www.fortiguard.com/webfilter/categories.

Potentially Liable

ID	Category
1	Drug Abuse
3	Hacking
4	Illegal or Unethical
5	Discrimination
6	Explicit Violence

ID	Category
12	Extremist Groups
59	Proxy Avoidance
62	Plagiarism
83	Child Abuse

Adult/Mature Content

ID	Category
2	Alternative Beliefs
7	Abortion
8	Other Adult Materials
9	Advocacy Organizations
11	Gambling
13	Nudity and Risque
14	Pornography
15	Dating

ID	Category
16	Weapons (Sales)
57	Marijuana
63	Sex Education
64	Alcohol
65	Tobacco
66	Lingerie and Swimsuit
67	Sports Hunting and War Games

Bandwidth Consuming

ID	Category
19	Freeware and Software Downloads
24	File Sharing and Storage
25	Streaming Media and Download
72	Peer-to-peer File Sharing
75	Internet Radio and TV
76	Internet Telephony

Security Risk

ID	Category
26	Malicious Websites
61	Phishing
	Newly Observed Domain
86	Spam URLs
88	Dynamic DNS
	Newly Registered Domain

Newly observed domain (NOD) applies to URLs whose domain name is not rated and were observed for the first time in the past 30 minutes.

Newly registered domain (NRD) applies to URLs whose domain name was registered in the previous 10 days.

General Interest - Personal

ID	Category
17	Advertising
18	Brokerage and Trading
20	Games
23	Web-based Email
28	Entertainment
29	Arts and Culture
30	Education
33	Health and Wellness
34	Job Search
35	Medicine
47	Travel
48	Personal Vehicles
54	Dynamic Content
55	Meaningless Content
58	Folklore
68	Web Chat
69	Instant Messaging
70	Newsgroups and Message Boards
71	Digital Postcards
77	Child Education

ID	Category
36	News and Media
37	Social Networking
38	Political Organizations
39	Reference
40	Global Religion
42	Shopping
44	Society and Lifestyles
46	Sports

ID	Category
78	Real Estate
79	Restaurant and Dining
80	Personal Websites and Blogs
82	Content Servers
85	Domain Parking
87	Personal Privacy
89	Auction

General Interest - Business

ID	Category
31	Finance and Banking
41	Search Engines and Portals
43	General Organizations
49	Business
50	Information and Computer Security
51	Government and Legal Organizations

ID	Category
52	Information Technology
53	Armed Forces
56	Web Hosting
81	Secure Websites
84	Web-based Applications

Local categories

Users can define custom or local categories. See Overriding FortiGuard Website Categorization for details.

FortiGuard web filtering usage quotas

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily quota by category, category group, or classification. Quotas allow access for a specified length of time or a specific bandwidth, calculated separately for each user. Quotas are reset every day at midnight.

Users must authenticate with the FortiGate unit. The quota is applied to each user individually so the FortiGate must be able to identify each user. One way to do this is to configure a security policy using the identity-based policy feature. Apply the web filter profile in which you have configured FortiGuard Web Filter and FortiGuard Web Filter quotas to such a security policy.

The use of FortiGuard Web Filtering quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a security policy in which user authentication is not required.

Editing the web filter profile resets the quota timers for all users.

When a user first attempts to access a URL, they're prompted to authenticate with the FortiGate unit. When they provide their user name and password, the FortiGate unit recognizes them, determines their quota allowances, and monitors their web use. The category and classification of each page they visit is checked and FortiGate unit adjusts the user's remaining available quota for the category or classification.

Quota hierarchy

You can apply quotas to categories and category groups. Only one quota per user can be active at any one time. The one used depends on how you configure the FortiGuard Web Filter.

When a user visits a URL, the FortiGate unit queries the FortiGuard servers for the category of the URL. From highest to lowest, the relative priority of the quotas are:

1. Category
2. Category group

Configuring web filter profiles

Enabling FortiGuard web filter

FortiGuard Web Filter is enabled and configured within web filter profiles by enabling FortiGuard Categories. The service is engaged by turning on the Web Filter profile and selecting a profile that has FortiGuard Categories enabled on one or more active policies being run by the firewall.

There is also a system wide setting for the enabling or disabling of FortiGuard Web Filter that is only in the CLI.

```
config system fortiguard
   set webfilter-force-off
```

The two options on this setting are enable or disable. The syntax of the settings name is "force-off" so in order to enable FortiGuard Webfilter you have to choose disable for the setting and enable if you want to turn it off.

General configuration steps

1. Go to **Security Profiles > Web Filter**.
2. Determine if you wish to create a new profile, edit an existing one, or clone and edit an existing one.
3. If you are using FortiGuard Categories, enable the FortiGuard Categories, select the categories and select the action to be performed.
4. Configure any **Category Usage Quotas** needed. (Proxy Mode)
5. Allow blocked override if required.(Proxy Mode)
6. Set up **Safe Search** settings and/or YouTube Education settings. (Proxy & Flow-based)
7. Configure **Static URL Settings**. (All Modes)
8. Configure **Rating Options**. (All Modes)

9. Configure **Proxy Options**.
10. Save the filter and web filter profile.
11. To complete the configuration, you need to select the security policy controlling the network traffic you want to restrict. Then, in the security policy, enable Web Filter and select the appropriate web filter profile from the list.

Configuring FortiGuard Web Filter settings

FortiGuard Web Filter includes a number of settings that allow you to determine various aspects of the filtering behavior.

Getting to the Edit Web Filter Profile configuration window

Once you have gotten to the profile configuration window there are a number of settings that can be used, most of which are optional. We will treat each of these options separately, but present the common instructions of how to get to the profile editing page here.

1. Go to **Security Profiles > Web Filter**.
2. Determine if you wish to create a new profile, edit an existing one, or clone and then edit an existing one.
   a. New profile:
      i. Select the **Create New** icon, in the upper right of the window (looks like a plus sign in a circle) **OR**
      ii. Select the **List** icon, in the upper right (looks like a white rectangle with lines like text). Select the **Create New** icon in the upper left.
   b. Edit existing profile:
      i. Select the name of the profile that you wish to edit from the drop-down menu **OR**
      ii. Select the **List** icon, in the upper right (looks like a white rectangle with lines like text. Highlight the name of the profile from the list and select **Edit** from the options above the list.
   c. Clone a profile:
      i. Select **Clone** icon in the upper right corner of the window (looks like one square overlapping another) **OR**
      ii. Select the **List**icon, in the upper right (looks like a white rectangle with lines like text. Highlight the name of the profile from the list and select **Clone** from the options above the list.
3. Make sure there is a valid name, and comment if you want.
4. Configure the settings to best achieve your specific requirements
5. Select **Apply** or **OK**, depending on whether you are editing, creating, or cloning a profile.

In older versions of FortiOS there was a character limitation for the URL of 2048 bytes or approximately 321 characters. If the URL you were trying to reach was longer the URL sent to FortiGuard would be truncated and the service would be unable to categorize the site. Starting in version 5 of the firmware, the parsed URL has been increase to 4 Kilobytes, effectively doubling the length of a URL capable of being categorized.

To configure the FortiGuard Web Filter categories

1. Go to the **Edit Web Filter Profile** window.

2. The category groups are listed in a widget. You can expand each category group to view and configure every sub-category individually within the groups. If you change the setting of a category group, all categories within the group inherit the change.
3. Select the category groups and categories to which you want to apply an action.
   To assign an action to a category left click on the category and select from the pop up menu.
4. Select **Apply** or **OK**.

Apply the web filter profile to an identity-based security policy. All the users subject to that policy are restricted by the quotas.

If you look at your logs carefully, you may notice that not every URL connection in the log shows a category. They are left blank. If you take one of those URL and enter it in the FortiGuard website designed to show the category for a URL it will successfully categorize it.

The reason for this is that to optimize speed throughput and reduce the load on the FortiGuard servers the FortiGate does not determine a category rating on scripts and css files.

Configuring FortiGuard Category quotas

1. Go to the **Edit Web Filter Profile** window
2. Verify that the categories that need to have quotas on them are set to one of these actions:
   - **Monitor**
   - **Warning**
   - **Authenticate**
3. Under **Category Usage Quota,** Select **Create New or Edit**
4. In the **New/Edit Quota** window that pops up, enable or disable the specific categories for that quota.
5. At the bottom of the widget, select a quota type and daily allowance for each user:
   - **Time** -- can be entered in **Hours**, **Minutes**, or **Seconds**.
   - **Traffic** -- can be entered in **Bytes**, **KB**, **MB**, or **GB** The value must be greater than 0.
6. Select **Apply or OK**.
7. Continue with any other configuration in the profile
8. Select **Apply or OK**.

Apply the web filter profile to an identity-based security policy. All the users subject to that policy are restricted by the quotas.

The use of FortiGuard Web Filtering quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a security policy in which user authentication is not required.

Editing the web filter profile resets the quota timers for all users.

Configure Allowed Blocked Overrides

1. Go to the **Edit Web Filter Profile window.**
2. Enable **Allow Blocked Override**

3. In the Apply to Group(s) field select the desired **User Group**
4. In the Assign to Profile field, select the desired profile

Configure search engine

There are 2 primary configuration settings in this section.

Enable SafeSearch

To enable the SafeSearch settings

1. Go to the **Edit Web Filter Profile window.**
2. Enable **SafeSearch**
3. Enable Search Engine SafeSearch
4. Enable YouTube Filter
   a. Enter the YouTube User ID in the Text field

Web Filter in flow mode does not support Safe Search

Log all search keywords

In the GUI, the configuration setting is limited to a checkbox.

Configure static URL filter

Web content filter

To enable the web content filter and set the content block threshold

1. Go to the **Edit Web Filter Profile window**.
2. In the **Static URL Filter section** enable **Web Content Filter**.
3. Select **Create New**.
4. Select the **Pattern Type**.
5. Enter the content **Pattern**.
6. Enter the **Language** from the dropdown menu.
7. Select **Block** or **Exempt**, as required, from the **Action** list.
8. Select **Enable**.
9. Select **OK.**

Configure rating options

Allow Websites When a Rating error Occurs

In the GUI, the configuration setting is limited to a checkbox.

Rate URLs by Domain and IP Address

In the GUI, the configuration setting is limited to a checkbox.

Block HTTP Redirects by Rating

In the GUI, the configuration setting is limited to a checkbox.

Rate Images by URL (Blocked images will be replaced with blanks)

In the GUI, the configuration setting is limited to a checkbox.

Configure Proxy Options

Restrict Google Account Usage to Specific Domains

Configuring the feature in the GUI

Go to **Security Profiles > Web Filter**.

In the **Proxy Options** section, check the box next to **Restrict to Corporate Google Accounts Only**.

Use the **Create New** link within the widget to add the appropriate Google domains that will be allowed.

Configuring the feature in the CLI

To configure this option in the CLI, the URL filter must refer to a web-proxy profile that is using the Modifying HTTP Request Headers feature. The command is only visible when the action for the entry in the URL filter is set to either allow or monitor.

1. Configure the proxy options:

```
config web-proxy profile
   edit "googleproxy"
      config headers
         edit 1
            set name "X-GoogApps-Allowed-Domains"
            set content "fortinet.com, Ladan.ca"
            end
         end
      end
   end
```

2. Set a web filter profile to use the proxy options

```
config webfilter urlfilter
   edit 1
      config entries
         edit "*.google.com"
            set type wildcard
            set action {allow | monitor}
            set web-proxy-profile <profile>
            end
         end
      end
   end
```

In the CLI, you can also add, modify, and remove header fields in HTTP request when scanning web traffic in proxy-mode. If a header field exists when your FortiGate receives the request, its content will be modified based on the configurations in the URL filter.

Web Resume Download block

In the GUI, the configuration setting is limited to a checkbox.

Provide Details for Blocked HTTP 4xx and 5xx Errors

In the GUI, the configuration setting is limited to a checkbox.

HTTP POST Action

Remove Java Applet Filter

In the GUI, the configuration setting is limited to a checkbox.

Remove ActiveX Filter

In the GUI, the configuration setting is limited to a checkbox.

Remove Cookie Filter

In the GUI, the configuration setting is limited to a checkbox.

Overriding FortiGuard website categorization

In most things there is an exception to the rule. When it comes to the rules about who is allowed to go to which websites in spite of the rules or in this case, policies, it seems that there are more exceptions than to most rules. There are numerous valid reasons and scenarios for exceptions so it follows that there needs to be a way to accommodate this exception.

The different methods of override

There are two different ways to override web filtering behavior based on FortiGuard categorization of a websites if you are operating in proxy-based inspection.

The second method has two variations in implementation and each of the three has a different level of granularity.

1. Using Alternate Categories
   Web Rating Overrides
   This method manually assigns a specific website to a different Fortinet category or a locally created category.
2. Using Alternate Profiles
   Administrative Override or Allow users to override blocked categories
   In this method all of the traffic going through the FortiGate unit, using identity based policies and a Web Filtering profile has the option where configured users or IP addresses can use an alternative Web Filter profile when attempting to access blocked websites.

Using Alternate Categories

Web Rating Overrides

There are two approaches to overriding the FortiGuard Web Filtering. The first is an identity-based method that can be configured using a combination of identity-based policies and specifically designed webfilter profiles. This is addressed in the Firewall Handbook.

The second method is the system-wide approach that locally (on the FortiGate Firewall) reassigns a URL to a different FortiGuard Category or even subcategory. This is where you can assign a specific URL to the FortiGuard Category that you want to you can also set the URL to one of the Custom Categories that you have created

The Web Rating Overrides option is available because different people will have different criteria for how they categorize websites. Even if the criteria is the same an organization may have reason to block the bulk of a category but need to be able to access specific URLs that are assigned to that category.

A hypothetical example could be that a website, example.com is categorized as being in the Sub-Category Pornography. The law offices of Barrister, Solicitor, and Lawyer do not want their employees looking at pornography at work so they have used the FortiGuard Webfilter to block access to sites that have been assigned to the Category “Pornography”. However, the owners of example.com are clients of the law office and they are aware that example.com is for artists that specialize in nudes and erotic images. In this case two approaches can be taken. The first is that the Web Rating Override function can be used to assign example.com to Nudity and Risque instead of Pornography for the purposes of matching the criteria that the law office goes by or the site can be assigned to a Custom Category that is not blocked because the site belongs to one of their clients and they always want to be able to access the site.

Another hypothetical example from the other side of the coin. A private school has decided that a company that specializes in the online selling of books that could be considered inappropriate for children because of their violent subject matter, should not be accessible to anyone in the school. The categorization by Fortinet of the site example2.com is General Interest - Business with the subcategory of Shopping and Auction, which is a category that is allowed at the school. In this case they school could reassign the site to the Category Adult Material which is a blocked category.

Local or Custom Categories

User-defined categories can be created to allow users to block groups of URLs on a per-profile basis. The categories defined here appear in the global URL category list when configuring a web filter profile. Users can rate URLs based on the local categories.

Users can create user-defined categories then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

Local categories and local rating features consume a large amount of CPU resources; use these features as little as possible.

The local assignment of a category overrides the FortiGuard server ratings and appear in reports as “Local” Categories or “Custom” Categories depending on the context.

CLI commands

In the CLI, the term is local category.

To create a local category:

```
config webfilter ftgd-local-cat
   edit local_category_1
      set id 140
   end
```

To set a rating to a Local Category:

```
config webfilter ftgd-local-rating
   edit <url_str>
      set rating {[<category_int>] [group_str] . . .]
      set status {enable | disable}
   end
```

GUI commands

In the GUI, **Local Categories** appears on the **Edit Web Filter** profile page and **Custom Categories** on the **Web Rating Overrides** page, if your FortiGate is in proxy-based or flow-based, profile-based inspection. If your FortiGate is operating with flow-based inspection and the policy-based NGFW mode, then you will not see the **Edit Web Filter** profile page.

Both these features will be used to create local categories and to apply actions to them.

Creating a Local or Custom Category

1. Go to **Security Profiles > Web Rating Overrides**.
2. Select **Custom Categories** in the top menu bar.
3. In the new window, click on **Create New**.
4. Enter the name of the custom category.
5. Select **OK**.

Configuring Web Rating Overrides

Using the GUI

1. Go to **Security Profiles > Web Rating Overrides.**
2. Select **Create New**
3. Type in the **URL** field the URL of the Website that you wish to recategorize. Do not use wildcard expressions when typing in the URL.
4. Select the **Lookup Rating** button to verify the current categorization assigned to the URL.
5. Change the **Category** field to one of the more applicable options from the drop down menu, for example, one of the custom categories just created.
6. Change the **Sub-Category** field to a more narrowly defined option within the main category.
7. Select **OK**.

It is usually recommended that you choose a category that you know will be addressed in existing Web Filter profiles so that you will not need to engage in further configuration.

Applying an Action to a Local or Custom Category

1. Go to **Security Profiles > Web Filter**.
2. Expand the **Local Categories** in the list of FortiGuard categories.
3. Right-click on a category from the list and set the action to **Allow**, **Block**, **Monitor**, **Warning**, **Authenticate**, or **Disable**.
4. Select **Apply**.

You cannot apply an action to a local category when operating in flow-based NGFW policy-based mode.

Web filtering local and remote category status

The `status` option allows you to enable or disable FortiGuard web filtering category overrides for local and remote categories. When disabled, `ssl-exempt`, `webfilter`, and `proxy-address` cannot use the category. The status cannot be set to `disable` if it has been referenced.

Syntax

```
config webfilter ftgd-local-cat
   edit <name>
      set status {disable | disable}
      set id 140
   next
end
```

Local Category scenarios

Scenario 1: The configuration of the domain name overrides the configuration for the subdirectory.

Depending on the URL specified or other aspects of configuration, the configuration of a local

or custom category may not take effect. Consider a scenario where you have defined:

- example.com – local rating as “category 1”, action set to Block
- example.com/subdirectory – local rating as “category 2”, action set to Monitor
- example.com/subdirectory/page.html – local rating as “category 3”, action set to Warning.

If a user browses to “example.com", access will be blocked. If a user browses to example.com/subdirectory, access will also be blocked,even though that address was configured to be part of category2. The configuration of the domain name overrides the configuration for the subdirectory.

However, if you configure a specific HTML page differently than the domain name, then that configuration will apply. In this scenario, the user will see a Warning message but will be able to pass through to the page.

Scenario 2: User-defined local ratings and SNI matches

In this scenario, local categories are defined and sites are added to those categories.

- There is no behavioral difference if the hostname is sent from from ClientHello SNI or from HTTP request-url.
- The SNI will be used as hostname for https certificate-inspection or ssl-exempt.
- If a valid SNI exist, then SNI will be used as the domain name for url rating instead of CN inthe server certificate.
- For the local rating, "example.com" will match "test.example.com", but will not match "another_example.com".

Using Alternate Profiles

Allow Blocked Overrides or Web Overrides

The Administrative Override feature for Web Filtering is found by going to **Security Profiles > Web Filter** and then enabling **Allow users to override blocked categories**.

The Concept

When a Web filter profile is overridden, it does not necessarily remove all control and restrictions that were previously imposed by the Web Filter. The idea is to replace a restrictive filter with a different one. In practice, it makes sense that this will likely be a profile that is less restrictive the original one but there is nothing that forces this. The degree to which the alternate profile is less restrictive is open. It can be as much as letting the user access everything on the Internet or as little as allowing only one addition website. The usual practice is to have as few alternate profiles as are needed to allow approved people to access what they need during periods when an exception to the normal rules is needed but still having enough control that the organizations web usage policies are not compromised.

You are not restricted to having only one alternative profile as an option to the existing profile. The new profile depends on the credentials or IP address making the connection. For example, John connecting through the "Standard" profile could get the "Allow_Streaming_Video" profile while George would get the "Allow_Social_Networking_Sites" profile.

The other thing to take into account is the time factor on these overrides. They are not indefinite. The longest that an override can be enabled is for 1 year less a minute. Often these overrides are set up for short periods of time for specific reasons such as a project. Having the time limitation means that the System Administrator does not have to remember to go back and turn the feature off after the project is finished.

Identity or Address

In either case, these override features -- for specified users, user groups or IP addresses -- allow sites blocked by Web Filtering profiles to be overridden for a specified length of time. The drawback of this method of override is that it takes more planning and preparation than the rating override method. The advantage is that once this has been set up, this method requires very little in the way of administrative overhead to maintain.

When planning to use the alternative profile approach keep in mind the following: In Boolean terms, one of the following "AND" conditions has to be met before overriding the Web Filter is possible.

Based on the IP address:

- The Web Filter profile must be specified as allowing overrides
- AND the user's computer is one of the IP addresses specified
- AND the time is within the expiration time frame.

While the conditions are fewer for this situation, there is less control over who has the ability to bypass the filtering configured for the site. All someone has to do is get on a computer that is allowed to override the Web Filter and they have access.

Based on user group:

- The Web Filter profile must be specified as allowing overrides
- AND the policy the traffic is going through must be identity based
- AND the user's credentials matches the identity credentials specified
- AND the time is within the expiration time frame.

This method is the one most likely to be used as it gives more control in that the user has to have the correct credential and is more versatile because the user can use the feature from any computer that uses the correct policy to get out on the Internet.

Settings

When using an alternate profile approach to Web Filter overrides, the following settings are used to determine authentication and outcome. Not every setting is used in both methods but enough of them are common to describe them collectively.

Apply to Group(s)

This is found in the Allow Blocked Overrides configuration. Individual users can not be selected. You can select one or more of the User Groups that are recognized my the FortiGate unit, whether they are local to the system or from a third part authentication device such as a AD server through FSSO.

Original Profile

This is found in the Administrative Override configuration. In the Allow Blocked Overrides setting the configuration is right inside the profile so there is no need to specify which profile is the original one, but the Administrative Override setup is done separately from the profiles themselves.

Assign to Profile or New Profile

Despite the difference in the name of the field, this is the same thing in both variations of the feature. You select from the drop down menu the alternate Web Filter Profile that you wish to set up for this override.

Scope or Scope Range

When setting up the override in the "Allow Blocked Overrides" variation, you are given a drop-down menu next to the field name Scope while in the Administrative Override configuration you are asked to select a radio button next to the same options. In both cases this is just a way of selecting which form of credentials will be required to approve the overriding of the existing Web Filter profile.

When the Web Filter Block Override message page appears it will display a field named "Scope:" and depending on the selection, it will show the type of credentials used to determine whether or not the override is allowed. The available options are:

- **User**
  This means that the authentication for permission to override will be based on whether or not the user is using a specific user account.

- **User Group**
  This means that the authentication for permission to override will be based on whether on not the user account supplied as a credential is a member of the specified User Group.

- **IP**
  This means that the authentication for permission to override will be based on the IP address of the computer that was used to authenticate. This would be used with computers that have multiple users. Example: If Paul logs on to the computer, engages the override using his credentials and then logs off, if the scope was based on the IP address of the computer, anybody logging in with any account on that computer would now be using the alternate override Web Filter profile.

  When entering an IP address in the Administrative Override version, only individual IP addresses are allowed.

  Differences between IP and Identity based scope

  - Using the IP scope does not require the use of an Identity based policy.
  - When using the Administrative Override variation and IP scope, you may not see a warning message when you change from using the original Web Filter profile to using the alternate profile. There is no requirement for credentials from the user so, if allowed, the page will just come up in the browser.
- **Ask**
  This option is available only in the "Allowed Blocked Overrides" variation and when used configures the message page to ask which scope the user wished to use. Normally, when the page appears the scope options are greyed out and not editable, but by using the ask option the option is dark and the user can choose from the choice of:
  - User
  - User Group
  - IP Address
- **Switch Duration**
  The Administrative Override sets a specified time frame that is always used for that override. The available options are:
  - **Predefined**
    Using this setting will mean that what ever is set as the duration will be the length of time that the override will be in effect. If the duration variable is set to 15 minutes the length of the override will always be 15 minutes. The option will be visible in the Override message page but the setting will be greyed out.
  - **Ask**
    Using this setting will give the person the option of setting the duration to the override when it is engaged. The user can set the duration in terms of Day, Hours and or Minutes.

- **Duration**
  Duration is one of the areas where the two variations take a different approach, on two aspects of the setting. As already indicated the "Administrative Override" only uses a static time frame there is no option for the user to select on the fly how long it will last. The other way in which the two variation differ is that the "Allow Blocked Overrides" starts the clock when the user logs in with his credentials. For example, if the duration is 1 hour and John initiates an override at 2:00 p.m. on January 1, at the end of that hour he will revert back to using the original profile but he can go back and re-authenticate and start the process over again. The Administrative override variation starts the clock from when the override was configured, which is why is shows an expiration date and time when your are configuring it.

  This option, which is available when the Switch Mode is set to Predefined is the time in minutes that the override will last when engaged by the user.

  When setting up a constant duration in the Web Based Interface, minutes is the only option for units of time. To set a longer time frame or to use the units of hours or days you can use the CLI.

```
config webfilter profile
   edit <name of webfilter profile>
      config override
         set ovrd-dur <###d##h##m>
      end
```

When configuring the duration you don't have to set a value for a unit you are not using. If you are not using days or hours you can use:

```
set ovrd-dur 30m
```

instead of:

```
set ovrd-dur 0d0h30m
```

However, each of the units of time variable has their own maximum level:

```
###d cannot be more than 364
##h cannot be more than 23
##m cannot be more than 59
```

So the maximum length that the override duration can be set to is 364 days, 23 hours, and 59 minutes.

Using cookies to authenticate users in a Web Filter override

Cookies can be used to authenticate users when a web filter override is used. This feature is available in CLI only.

CLI syntax:

```
config webfilter cookie-ovrd
   set redir-host <name or IP>
   set redir-port <port>
end

config webfilter profile
   edit <name>
      config override
         set ovrd-cookie [allow | deny]
         set ovrd-scope [user | user-group | ip | ask]
         set profile-type [list | radius]
         set ovrd-dur-mode [constant | ask]
         set ovrd-dur <duration>
         set ovrd-user-group <name>
         set profile <name>
      end
   end
end
```

Threat Feed Connectors

This feature introduces the ability to dynamically import external block list text files from an HTTP server. The text files can contain IP addresses and domain names. These dynamic block lists are called 'Threat Feeds'. You can block access to the addresses in the text files by adding one or more threat feeds to:

- DNS Filter profiles (using Domain Name and IP Address threat feeds)
- Web Filter profiles and SSL inspection exemptions (using FortiGuard Category threat feeds)

- Proxy policies (using IP Address threat feeds)
- AntiVirus profiles (using Malware Hash threat feeds)

FortiOS keeps threat feeds up to date by dynamically re-downloading them from the HTTP server according to the refresh rate.

Threat Feeds can be configured under **Security Fabric > Fabric Connectors**by creating new **Threat Feeds**.

The **New Fabric Connector** edit page provides the following fields:

- **Name** - The name you want to assign to the feed. The usage of the name in the interface depends on the category of threat feed you select:
  - **Domain Name** - The **Name** will appear as an "Remote Category" in DNS Filter profiles.
  - **FortiGuard Category** - The **Name** will appear as a "Remote Category" in Web Filter profiles and SSL inspection exemptions.
  - **IP Address** - The **Name** will appear as an "External IP Block List" in DNS Filter profiles and as a "Source/Destination" in IPv4, IPv6, and Proxy policies.
  - **Malware Hash** - The **Name** will be automatically used for Virus Outbreak Prevention on AntiVirus Profiles where "External Malware Block List" is enabled.
- **URI of external resource** - The link to an external resource file. The file should be a plain text file with one domain each line and supports simple wildcard.
- **HTTP basic authentication** - The username and password for external authentication on the threat feed's URI. This can be disabled if the feed does not require authentication.
- **Refresh Rate** - The time interval to refresh external resource (1 - 43200 minutes).
- The size of the file can be 10 MB, or 128,000 lines of text, whichever is most restrictive.

The domain resource is a text file which contains a domain name for each line and supports simple wildcard. For example:

mail.*.or.th
*-special.de.vu
http://www.*de.vu
610-pawn.com
aaliyah-hq-gallery.de.vu
abcgolocal.com

The address resource is a text file which contains an IP/IP range for each line (note that only IPv4 is supported in DNS profiles, so IPv6 addresses will be ignored). For example:

1.1.1.1
10.0.0.70
2.1.1.1
100.0.0.1-100.0.0.100
10.0.0.99-10.0.0.201
1.2.2.2/24

Syntax

```
config system external-resource
   edit <name>
      set type {category | address | domain}
      set category <value>
      set comments [comments]
```

```
        set resource <resource-url>
        set refresh-rate <minutes>
        set last-update <datetime>
    next
end
```

You can also configure one or more domain list threat feeds under `config dnsfilter profile`. See "DNS Filter " on page 1 for more information.

Web Profile Overrides

This feature allows administrators to grant temporary access to sites that are otherwise blocked by a web filter profile. The temporary access can be granted to a user, user group, or source IP address. The time limit can be set in days, hours, or minutes. The default is 15 minutes.

Temporary access can also be granted to a user, user group, or source IP address by enabling **Allow users to override blocked categories** in a Web Filter security profile and applying that profile to the appropriate policy. In this scenario, the user will have to authenticate to gain access.

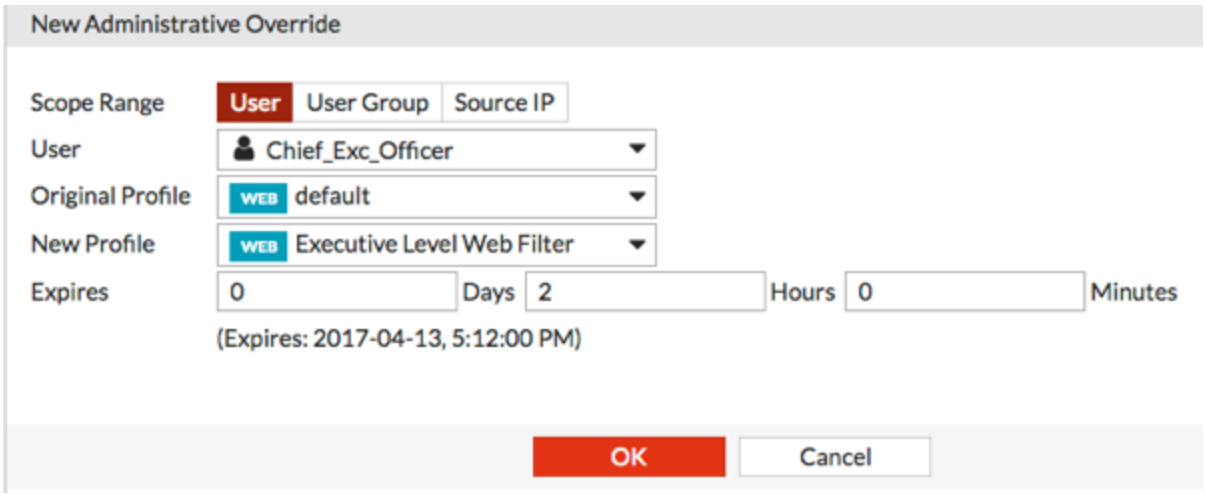
When Web Profile Overrides is in effect, a blocked access page or replacement message will not appear and authentication will not be required.

If your FortiGate is operating in flow-based inspection and policy-based NGFW mode, then you cannot create a web profile override.

Creating a Web Profile Override

Before creating a Web Profile Override, you will have to configure a user or user group if not granting temporary access to a Source IP. You will also have to configure the Web Filter security profile to be applied to the override.

1. Go to **Security Profiles > Web Profile Overrides.**
2. Select **Create New**.



3. Select:
   - The **Scope Range**: **User** and **User Group** should be previously configured under **User & Device**
   - The **Original Profile** that applied to the scope range.
   - The **New Profile** to apply for the override
   - The time when the override **Expires**; default is 15 minutes

SafeSearch

SafeSearch is a feature of popular search sites that prevents explicit web sites and images from appearing in search results. Although SafeSearch is a useful tool, especially in educational environments, the resourceful user may be able to simply turn it off. Enabling SafeSearch for the supported search sites enforces its use by rewriting the search URL to include the code to indicate the use of the SafeSearch feature. For example, on a Google search it would mean adding the string “&safe=active” to the URL in the search.

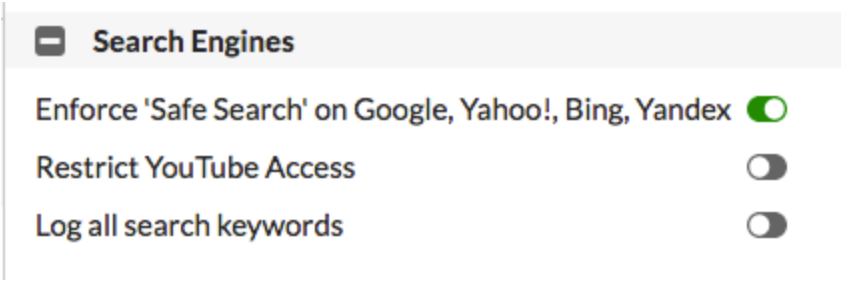
The search sites supported are:

- Google
- Yahoo
- Bing
- Yandex

You can only enable SafeSearch with proxy-based inspection mode.

Enabling SafeSearch - GUI

1. Go to **Security Profiles > Web Filter** and edit or create a policy.
2. Expand **Search Engines**



Enabling SafeSearch - CLI

```
config webfilter profile
   edit default
      config web
         set safe-search <url>
      end
   end
```

This enforces the use of SafeSearch in traffic controlled by the firewall policies using the web filter you configure.

Search Keywords

There is also the capability to log the search keywords used in the search engines.

YouTube Education Filter

YouTube for Schools was a way to access educational videos from inside a school network. This YouTube feature gave schools the ability to access a broad set of educational videos on YouTube EDU and to select the specific videos that are accessible from within the school network.

Google stopped supporting YouTube for Schools (YTfS) as of July 1, 2016. Consequently, the current YouTube safe search does not work anymore.

Google provides an article entitled "Restrict YouTube content on your network or managed devices" on its support site. At this time, Google offers two options to restrict inappropriate content: DNS and HTTP header.

To restrict YouTube access, go to **Security Profiles > Web Filter**, scroll to **Search Engines** and enable **Restrict YouTube Access**. You can select either **Strict** or **Moderate** level of restriction. Your FortiGate must be in proxy mode.

YouTube Channel Filtering

This Web Filtering feature lets you block or allow matched YouTube channels using one of the following identifiers:

- **<channel-id>**
- **www.youtube.com/channel/<channel-id>**
- **www.youtube.com/user/<user-id>**
  matches channel-id from <meta itemprop="channelId" content="UCGzuiiLdQZu9wxDNJHO_JnA">
- **www.youtube.com/watch?v=<string>**
  matches channel-id from <meta itemprop="channelId" content="UCGzuiiLdQZu9wxDNJHO_JnA">

Syntax

Note that `config youtube-channel-filter` is only available when `youtube-channel-status` is set to either `blacklist` or `whitelist`. Also note that, when defining `channel-id`, both the full URL or just the Channel ID suffix are acceptable, as shown below:

```
config webfilter profile
   edit <name>
      set youtube-channel-status {disable | blacklist | whitelist}
      config youtube-channel-filter
         edit <id>
            set channel-id <url>
         next
         edit <id>
            set channel-id <channel-id>
         next
   end
end
```

Static URL filter

You can allow or block access to specific URLs by adding them to the **Static URL Filter** list. The filter allows you to block, allow, or monitor URLs by using patterns containing text, regular expressions, or wildcard characters. The FortiGate unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to ftp:// ftp.example.com. Instead, use firewall policies to deny ftp connections.

When adding a URL to the URL filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls access to the news page on this web site.
- To control access to all pages with a URL that ends with example.com, add `example.com` to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.
- Control access to all URLs that match patterns using text and regular expressions (or wildcard characters). For example, `example.*` matches example.com, example.org, example.net and so on.

URLs with an action set to exempt or monitor are not scanned for viruses. If users on the network download files through the FortiGate unit from a trusted web site, add the URL of this web site to the URL filter list with an action to pass it so the FortiGate unit does not virus scan files downloaded from this URL.

URL formats

How URL formats are detected when using HTTPS

Filter HTTPS traffic by entering a top level domain name, for example, `www.example.com` if:

- your unit does not support SSL content scanning and inspection
- you have selected the **URL filtering** option in web content profile for **HTTPS content filtering mode** under **Protocol Recognition**.

HTTPS URL filtering of encrypted sessions works by extracting the CN from the server certificate during the SSL negotiation. Since the CN only contains the domain name of the site being accessed, web filtering of encrypted HTTPS sessions can only filter by domain names.

If your unit supports SSL content scanning and inspection and if you have selected Deep Scan, you can filter HTTPS traffic in the same way as HTTP traffic.

How URL formats are detected when using HTTP

URLs with an action set to Exempt are not scanned for viruses. If users on the network download files through the unit from trusted web site, add the URL of this web site to the URL filter list with an action set to exempt so the unit does not virus scan files downloaded from this URL.

- Type a top-level URL or IP address to control access to all pages on a web site. For example, `www.example.com` or `192.168.144.155` controls access to all pages at this web site.
- Enter a top-level URL followed by the path and filename to control access to a single page on a web site. For example, `www.example.com/news.html` or `192.168.144.155/news.html` controls the news page on this web site.
- To control access to all pages with a URL that ends with `example.com`, add `example.com` to the filter list. For example, adding `example.com` controls access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.
- Control access to all URLs that match patterns created using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on.
- Fortinet URL filtering supports standard regular expressions.

If virtual domains are enabled on the unit, web filtering features are configured globally. To access these features, select **Global Configuration** on the main menu.

URL filter actions

You can select one of four actions for how traffic will be treated as it attempts to reach a site in the list.

Block

Attempts to access any URLs matching the URL pattern are denied. The user will be presented with a replacement message.

Allow

Any attempt to access a URL that matches a URL pattern with an allow action is permitted. The traffic is passed to the remaining antivirus proxy operations, including FortiGuard Web Filter, web content filter, web script filters, and antivirus scanning.

Allow is the default action. If a URL does not appear in the URL list, it is permitted.

Monitor

Traffic to, and reply traffic from, sites matching a URL pattern with **Monitor** action applied will be allowed through in the same way as the **Allow** action. The difference with the **Monitor** action is that a log message will be generated each time a matching traffic session is established. The requests will also be subject to all other Security Profiles inspections that would normally be applied to the traffic.

Exempt

Exempt allows trusted traffic to bypass the antivirus and DLP proxy operations by default, but it functions slightly differently. In general, if you're not certain that you need to use the **Exempt** action, use **Monitor**.

Using the static URL filter to exempt scanning also prevents SSL inspection.

HTTP 1.1 connections are persistent unless declared otherwise. This means the connections will remain in place until closed or the connection times out. When a client loads a web page, the client opens a connection to the web server. If the client follows a link to another page on the same site before the connection times out, the same connection is used to request and receive the page data.

When you add a URL pattern to a URL filter list and apply the **Exempt** action, traffic sent to and replies traffic from sites matching the URL pattern will bypass all antivirus proxy operations. The connection itself inherits the exemption. This means that all subsequent reuse of the existing connection will also bypass all antivirus proxy operations. When the connection times out, the exemption is cancelled.

For example, consider a URL filter list that includes `example.com/files` configured with the **Exempt** action. A user opens a web browser and downloads a file from the URL `example.com/sample.zip`. This URL does not match the URL pattern so it is scanned for viruses. The user then downloads `example.com/files/beautiful.exe` and since this URL does match the pattern, the connection itself inherits the exempt action. The user then downloads `example.com/virus.zip`. Although this URL does not match the exempt URL pattern, a previously visited URL did, and since the connection inherited the exempt action and was re-used to download a file, the file is not scanned.

If the user next goes to an entirely different server, like `example.org/photos`, the connection to the current server cannot be reused. A new connection to example.org is established. This connection is not exempt. Unless the user goes back to example.com before the connection to that server times out, the server will close the connection. If the user returns after the connection is closed, a new connection to example.com is created and it is not exempt until the user visits a URL that matches the URL pattern.

Web servers typically have short time-out periods. A browser will download multiple components of a web page as quickly as possible by opening multiple connections. A web page that includes three photos will load more quickly if the browser opens four connections to the server and downloads the page and the three photos at the same time. A short time-out period on connections will close the connections faster, allowing the server to avoid

unnecessarily allocating resources for a long period. The HTTP session time-out is set by the server and will vary with the server software, version, and configuration.

Using the **Exempt** action can have unintended consequences in certain circumstances. You have a web site at example.com and since you control the site, you trust the contents and configure `example.com` as exempt. But example.com is hosted on a shared server with a dozen other different sites, each with a unique domain name. Because of the shared hosting, they also share the same IP address. If you visit example.com, your connection your site becomes exempt from any antivirus proxy operations. Visits to any of the 12 other sites on the same server will reuse the same connection and the data you receive is exempt from being scanned.

Use of the **Exempt** action is not suitable for configuration in which connections through the FortiGate unit use an external proxy. For example, you use proxy.example.net for all outgoing web access. Also, as in the first example, URL filter list that includes a URL pattern of `example.com/files` configured with the **Exempt** action. Users are protected by the antivirus protection of the FortiGate unit until a user visits a URL that matches the of `example.com/files` URL pattern. The pattern is configured with the **Exempt** action so the connection to the server inherits the exemption. With a proxy however, the connection is from the user to the proxy. Therefore, the user is entirely unprotected until the connection times out, no matter what site he visits.

Ensure you are aware of the network topology involving any URLs to which you apply the **Exempt** action.

Status

The Web Site Filter has the option to either enable or disable individual web sites in the list. This allows for the temporary removal of the actions against a site so that it can be later reengaged without having to rewrite the configuration.

Configuring a URL filter

Consult the Maximum Values Table on the Fortinet Document Library site for up-to-date information on the number of URL filter entries allowed for your FortiGate.

You can only set a Static URL Filter with proxy-based inspection mode and flow-based inspection mode in profile-based NGFW mode.

For this example, the URL www.example*.com will be used. You configure the list by adding one or more URLs to it.

To add a URL to a URL filter

1. Go to **Security Profiles > Web Filter**.
2. Create a new web filter or select a one to edit.
3. Expand **Static URL Filter**, enable **URL Filter**, and select **Create**.
4. Enter the URL, without the “http”, for example: `www.example*.com`.
5. Select a **Type**: **Simple** , **Reg. Expression**, or **Wildcard**. In this example, select **Wildcard**.
6. Select the **Action** to take against matching URLs: **Exempt**, **Block**, **Allow**, or **Monitor**.
7. Confirm that **Status** is enabled.
8. Select **OK**.

'Simple' Filter type

If you select the **Simple** filter type for a URL filter, the syntax is performing an exact match. Note, however, that the domain and path are separate entities in HTTP despite the fact that a user types them as a single entity and, in the case of 'simple', the rules for each part (domain and path) are different.

The 'domain' part

For the domain part, the goal of the 'simple' format is to make it easy to block a domain and all its subdomains, such that the admin only has to type “address.xy" to block "address.xy", "www.address.xy", "talk.address.xy", etc. but *not* block “youraddress.xy" or "www.youraddress.xy" which are different domains from "address.xy”.

Also, the actual domain does not include http:// or https:// so this should *not* be entered or the URL filter will try to match a domain starting with http. For this reason, when you enter http:// in the URL filter via the GUI, it is automatically removed.

A trailing ‘/‘ with the domain is not needed. The GUI URL filter will automatically trim this, but when using the API to provide the per-user BWL it will not!

Please take this into account. Better not to use it as it might give unexpected results.

The 'path' part

For the path part, an exact match takes place. For example:

www.address.xy/news

blocks anything that starts with that exact path. So this matches:

www.address.xy/newsies
www.address.xy/newsforyou
www.address.xy/news/co
etc.

Also:

www.address.xy/new

likewise blocks the same as above but includes:

/newt
/newp
etc.

which is a much broader filter, matching:

www.address.xy/newstand/co
www.address.xy/news/co
etc.

In other words, the more you specify of the path, the more strictly it will match.

Here as well a trailing '/' with the URL path is not needed, the GUI URL filter will automatically trim this, but when using the API to provide the per-user BWL it will not!

Please take this into account. Better not to use it as it might give unexpected results.

Referrer URL

A new variable has been added to the Static URL Filter: `referrer-host`. If a referrer is specified, the hostname in the referrer field of the HTTP require will be compared for any entry that contains the matching URL. If the referrer matches, then the specified action will be performed by proxy.

Configuring in the GUI

The configuration can be done in the GUI but only if advance web filtering features have been enabled by entering the following commands in the CLI:

```
config system global
   set gui-webfilter-advanced enable
end
```

After this command is used, a new column will be created in **Security Profiles > Web Filter** to set the referrer.

Configuring in the CLI

When specifying the URL filter, it needs to be identified by its ID. The URLs are listed under each entry.

To find the ID number:

```
config webfilter urlfilter
   edit ?
```

A list of the current URL filters will be listed with their ID numbers in the left column.

The syntax in the CLI for configuring an entry is:

```
config webfilter urlfilter
   edit <ID>
      config entries
         edit 1
            set url <url>
            set referrer-host <url>
            set type {simple | regex | wildcard}
            set action {block | allow | monitor | exempt}
            set status {enable | disable}
         end
      end
   end
```

Web content filter

You can control web content by blocking access to web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can also add words, phrases, patterns, wild cards and

Perl regular expressions to match content on web pages. You can add multiple web content filter lists and then select the best web content filter list for each web filter profile.

Enabling web content filtering involves three separate parts of the FortiGate configuration.

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day.
- The web filter profile specifies what sort of web filtering is applied.
- The web content filter list contains blocked and exempt patterns.

The web content filter feature scans the content of every web page that is accepted by a security policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases in the page. If the sum is higher than a threshold set in the web filter profile, the FortiGate unit blocks the page.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a web content filter list.
2. Add patterns of words, phrases, wildcards, and regular expressions that match the content to be blocked or exempted.
3. You can add the patterns in any order to the list. You need to add at least one pattern that blocks content.
4. In a web filter profile, enable the web content filter and select a web content filter list from the options list.

To complete the configuration, you need to select a security policy or create a new one. Then, in the security policy, enable **Webfilter** and select the appropriate web filter profile from the list.

Creating a web filter content list

You can create multiple content lists and then select the best one for each web filter profile. Creating your own web content lists can be accomplished only using the CLI.

This example shows how to create a web content list called inappropriate language, with two entries, offensive and rude.

To create a web filter content list

```
config webfilter content
   edit 3
      set name "inappropriate language"
      config entries
         edit offensive
            set action block
            set lang western
            set pattern-type wildcard
            set score 15
            set status enable
         next
         edit rude
            set action block
            set lang western
            set pattern-type wildcard
```

```
            set score 5
            set status enable
        end
    end
end
```

Configuring a web content filter list

Once you have created the web filter content list, you need to add web content patterns to it. There are two types of patterns: **Wildcard** and **Regular Expression**.

You use the **Wildcard** setting to block or exempt one word or text strings of up to 80 characters. You can also use the wildcard symbols, such as “*” or “?”, to represent one or more characters. For example, as a wildcard expression, forti*.com will match fortinet.com and forticare.com. The “*” represents any kind of character appearing any number of times.

You use the **Regular Expression** setting to block or exempt patterns of Perl expressions, which use some of the same symbols as wildcard expressions, but for different purposes. The “*” represents the character before the symbol. For example, forti*.com will match fortiii.com but not fortinet.com or fortiice.com. The symbol “*” represents “i” in this case, appearing any number of times. RP: Add a regex example.

The maximum number of web content patterns in a list is 5000.

How content is evaluated

Every time the web content filter detects banned content on a web page, it adds the score for that content to the sum of scores for that web page. You set this score when you create a new pattern to block the content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the sum of scores equals or exceeds the threshold score, the web page is blocked. The default score for web content filter is 10 and the default threshold is 10. This means that by default a web page is blocked by a single match. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

Banned words or phrases are evaluated according to the following rules:

- The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.
- The score for any word in a phrase without quotation marks is counted.
- The score for a phrase in quotation marks is counted only if it appears exactly as written.

The following table describes how these rules are applied to the contents of a web page. Consider the following, a web page that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.”

Banned pattern rules

Banned pattern	Assigned score	Score added to the sum for the entire page	Threshold score	Comment
word	20	20	20	Appears twice but only counted once. Web page is blocked.
word phrase	20	40	20	Each word appears twice but only counted once giving a total score of 40. Web page is blocked
word sentence	20	20	20	“word” appears twice, “sentence” does not appear, but since any word in a phrase without quotation marks is counted, the score for this pattern is 20. Web page is blocked.
“word sentence”	20	0	20	“This phrase does not appear exactly as written. Web page is allowed.
“word or phrase”	20	20	20	This phrase appears twice but is counted only once. Web page is blocked.

Enabling the web content filter and setting the content threshold

When you enable the web content filter, the web filter will block any web pages when the sum of scores for banned content on that page exceeds the content block threshold. The threshold will be disregarded for any exemptions within the web filter list.

Web filtering example

Web filtering is particularly important for protecting school-aged children. There are legal issues associated with improper web filtering as well as a moral responsibility to keep children from viewing inappropriate material. The key is to design a web filtering system in such a way that students and staff do not fall under the same web filter profile in the FortiGate configuration. This is important because the staff may need to access websites that are off limits to the students.

School district

The background for this scenario is a school district with more than 2,300 students and 500 faculty and staff in a preschool, three elementary schools, a middle school, a high school, and a continuing education center. Each elementary school has a computer lab and the high school has three computer labs with connections to the Internet. Such easy access to the Internet ensures that every student touches a computer every day.

With such a diverse group of Internet users, it was not possible for the school district to set different Internet access levels. This meant that faculty and staff were unable to view websites that the school district had blocked. Another issue was the students’ use of proxy sites to circumvent the previous web filtering system. A proxy server

acts as a go-between for users seeking to view web pages from another server. If the proxy server has not been blocked by the school district, the students can access the blocked website.

When determining what websites are appropriate for each school, the district examined a number of factors, such as community standards and different needs of each school based on the age of the students.

The district decided to configure the FortiGate web filtering options to block content of an inappropriate nature and to allow each individual school to modify the options to suit the age of the students. This way, each individual school was able to add or remove blocked sites almost immediately and have greater control over their students' Internet usage.

In this simplified example of the scenario, the district wants to block any websites with the word **example** on them, as well as the website www.example.com. The first task is to create web content filter lists for the students and the teachers.

Web Filter in flow mode does not support Safe Search. The examples below use Web Filter in proxy mode.

Create a Web Filter profile for the students

1. Go to **Security Profiles > Web Filter**.
2. Select the **Create New** icon.
3. Enter the name "Students" in the name field.
4. Enable FortiGuard Categories.
   a. Set the following categories to **Block**:
   - Potentially Liable
   - Adult/Mature Content
   - Security Risk

URL Content

6. Go to **Search Engines** and expand the section if necessary. Enable **Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex**
7. In the **Static URL Filter** section, enable **URL Filter**.
   a. Select **Create New**.
      i. In the **URL** field, enter *example*.*
      ii. For the **Type** field, select **Wildcard**
      iii. For the **Action** field, select **Block**
      iv. For the **Status** field, check **enable**
      v. Select **OK**

Web Content Filter

8. In the **Static URL Filter** section, enable **Web Content Filter**.
   a. In the **Web Content Filter** widget, select **Create New**.
      i. For the **Pattern Type** field, select **Reg. Expression**
      ii. In the **Pattern** field, enter "example"
      iii. For the **Language** field, choose Western

iv. For the **Action** field, select “Block”
v. For the **Status** field, check Enable.
vi. Select **OK**

9. Enable**Rate URLs by Domain and IP Address**
10. Disable **Allow websites when a rating error occurs** .
11. Check **Rate Images by URL (Blocked images will be replaced with blanks)**
12. Select **Apply**

Create a Web Filter for the teachers

It might be more efficient if the Teacher Web Content List included the same blocked content as the student list. From time to time a teacher might have to view a blocked page. It would then be a matter of changing the **Action** from **Block** to **Allow** as the situation required. The following filter is how it could be set up for the teachers to allow them to see the “example” content if needed while keeping the blocking inappropriate material condition.

1. Go to **Security Profiles > Web Filter**.
2. Select the **Create New** icon.
3. Enter the name “Teachers” in the name field.
4. Enable FortiGuard Categories.
   a. Set the following categories to **Block**:
   - Potentially Liable
   - Adult/Mature Content
   - Security Risk

URL Content

6. Go to **Search Engines** and expand the section if necessary. Enable **Search Engine Safe Search on Google, Yahoo!, Bing, Yandex**.
7. In the Static URL Filter section, check **Enable URL Filter**.
   a. Select **Create New**.
      i. In the **URL** field, enter *example*.*
      ii. For the **Type** field, select **Wildcard**
      iii. For the **Action** field, select Block
      iv. For the **Status** field, check enable
      v. Select **OK**

Web Content Filter

8. In the Static URL Filter section, check Enable Web Content Filter.
   a. In the Web Content Filter widget, select **Create New**.
   b. Enter the name “Teachers” in the name field.
      i. For the **Pattern Type** field, select **Reg. Expression**
      ii. In the **Pattern** field, enter “example”
      iii. For the **Language** field, choose Western
      iv. For the **Action** field, select Exempt

v. For the **Status** field, check Enable.
vi. Select **OK**

9. Check **Rate URLs by Domain and IP Address**
10. Check **Rate Images by URL (Blocked images will be replaced with blanks)**
11. Select **OK**

To create a security policy for the students

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select the policy being used to manage student traffic.
3. Enable **Web Filter**.
4. Select **Students** from the web filter drop-down list.
5. Select **OK**.

To create a security policy for Teachers

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select the policy being used to manage teacher traffic.
3. Enable **Web Filter**.
4. Select **Teachers** from the web filter drop-down list.
5. Select **OK**.
6. Make sure that the student policy is in the sequence before the teachers' policy.

Advanced web filter configurations

Allow websites when a rating error occurs

Enable this setting to allow access to web pages that return a rating error from the FortiGuard Web Filter service.

If your FortiGate unit cannot contact the FortiGuard service temporarily, this setting determines the tye of access the FortiGate unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.

ActiveX filter

Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX may not function properly with this filter enabled.

Block HTTP redirects by rating

Enable to block HTTP redirects.

Many web sites use HTTP redirects legitimately but in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.

This option is not supported for HTTPS.

Block Invalid URLs

Select to block web sites when their SSL certificate CN field does not contain a valid domain name.

FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is not selected, the following behavior occurs:

- If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name.
- If the request is to a web server proxy, the real IP address of the web server is not known. Therefore, rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.

Enabling the Web Filter profile to block a particular category and enabling the Application Control profile will not result in blocking the URL. This occurs because proxy and flow-based profiles cannot operate together.

To ensure replacement messages show up for blocked URLs, switch the Web Filter to flow-based inspection.

Cookie filter

Enable to filter cookies from web traffic. Web sites using cookies may not function properly with this enabled.

Provide Details for Blocked HTTP 4xx and 5xx Errors

Enable to have the FortiGate unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.

HTTP POST action

Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.

The available actions include:

Comfort

Use client comforting to slowly send data to the web server as the FortiGate unit scans the file. Use this option to prevent a server time-out when scanning or other filtering is enabled for outgoing traffic.

The client comforting settings used are those defined in the Proxy Options profile selected in the security policy.

Block

Block the HTTP POST command. This will limit users from sending information and files to web sites.

When the post request is blocked, the FortiGate unit sends the http-post-block replacement message to the web browser attempting to use the command.

Java applet filter

Enable to filter java applets from web traffic. Web sites using java applets may not function properly with this filter enabled.

Rate Images by URL

Enable to have the FortiGate retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category.

Blocked images are replaced on the originating web pages with blank place-holders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.

Rate URLs by Domain and IP Address

Enable to have the FortiGate unit request the rating of the site by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter.

If the rating determined by the domain name and the rating determined by the IP address defer the Action that is enforce will be determined by a weighting assigned to the different categories. The higher weighted category will take precedence in determining the action. This will have the side effect that sometimes the Action will be determined by the classification based on the domain name and other times it will be determined by the classification that is based on the IP address.

FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This can sometimes cause the FortiGate unit to allow access to sites that should be blocked, or to block sites that should be allowed.

An example of how this would work would be if a URL's rating based on the domain name indicated that it belonged in the category Lingerie and Swimsuit, which is allowed but the category assigned to the IP address was Pornography which has an action of Block, because the Pornography category has a higher weight the effective action is Block.

Web resume download block

Enable to prevent the resumption of a file download where it was previously interrupted. With this filter enabled, any attempt to restart an aborted download will download the file from the beginning rather than resuming from where it left off.

This prevents the unintentional download of viruses hidden in fragmented files.

Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may also break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.

Restrict Google account usage to specific domains

This feature allow the blocking of access to some Google accounts and services while allowing access to accounts that are included in the domains specified in the exception list.

Block non-English character URLs

The FortiGate will not successfully block non-English character URLs if they are added to the URL filter. In order to block access to URLs with non-English characters, the characters must be translated into their international characters.

Browse to the non-English character URL (for example, http://www.fortinet.com/pages/ที่นี่-ไม่มีเศษรัฐประหารให้ใครแดก/338419686287505?ref=stream).

On the FortiGate, use the URL shown in the FortiGate GUI and add it the list of blocked URLs in your URL filter (for example, http://www.fortinet.com/pages/%E0%B8%97%E0%B8%B5%E0%B9%88%E0%B8%99%E0%B8%B5%E0%B9%88-%E0%B9%84%E0%B8%A1%E0%B9%88%E0%B8%A1%E0%B8%B5%E0%B9%80%E0%B8%A8%E0%B8%A9%E0%B8%A3%E0%B8%B1%E0%B8%90%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%AB%E0%B8%B2%E0%B8%A3%E0%B9%83%E0%B8%AB%E0%B9%89%E0%B9%83%E0%B8%84%E0%B8%A3%E0%B9%81%E0%B8%94%E0%B8%81/338419686287505?ref=stream).

Once added, further browsing to the URL will result in a blocked page.

CLI Syntax

```
config webfilter urlfilter
   edit 1
      set name "block_international_character_urls"
         config entries
            edit 1
               set url "www.fortinet.com/pages/2.710850E-3120%B8%E0%B8%B53.231533E-
                   3170%B9%E0%B8%E0%B8%B53.231533E-3170%B9%88-3.230415E-
                   3170%B9%E0%B80X0.000000063CD94P-102211.482197E-
                   3230%B9%E0%B80X0.0007FBFFFFCFP-102210.000000E+000%B8%B51.828043E-
                   3210%B9%E0%B80X0P+081.828043E-3210%B80X0P+092.710850E-
                   3120%B80X0.0000000407ED2P-102233.236834E-3170%B8%B19.036536E-
                   3130%B8%E0%B8%9B4.247222E-3140%B80X0P+039.036683E-3130%B8%B02.121996E-
                   3130%B80X0.0000000000008P-1022B2.710850E-3120%B8%B21.482197E-
                   3230%B80X0P+030.000000E+000%B9%E0%B80X0P+0B2.710850E-
                   3120%B9%E0%B9%E0%B8%E0%B80X0.0000000408355P-102232.023693E-
                   3200%B9%E0%B8%E0%B8%81/338419686287505?ref=stream"
               set action block
            next
         end
   next
end

config webfilter urlfilter
   edit 2
      set name "block_international_character_urls"
   next
end

config webfilter profile
   edit "block_international_character_urls"
   next
end

config firewall policy
   edit 3
```

```
        set uuid cf80d386-7bcf-51e5-6e87-db207e3f0fa8
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set webfilter-profile "block_international_character_urls"
        set profile-protocol-options "default"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
    next
end
```

Websense web filtering through WISP

WISP is a Websense protocol that allows for URLs to be extracted by a firewall and submitted to Websense systems for rating and approval checking.

This feature provides a solution for customers who have large, existing, deployed implementations of Websense security products to replace their legacy firewalls with a FortiGate family, such that they are not forced to make a change to their web filtering infrastructure at the same time.

When WISP is enabled, the FortiGate will maintain a pool of TCP connections to the WISP server. The TCP connections will be used to forward HTTP request information and log information to the WISP server and receive policy decisions.

Configuring the WISP server

In order to use WebSense's web filtering service, a WISP server per VDOM must be defined and enabled first.

```
config web-proxy wisp
    edit {name}
    # Configure Wireless Internet service provider (WISP) servers.
        set name {string}   Server name. size[35]
        set comment {string}   Comment. size[255]
        set outgoing-ip {ipv4 address any}   WISP outgoing IP address.
        set server-ip {ipv4 address any}   WISP server IP address.
        set server-port {integer}   WISP server port (1 - 65535, default = 15868). range[1-65535]
        set max-connections {integer}   Maximum number of web proxy WISP connections (4 - 4096, default =
64). range[4-4096]
        set timeout {integer}   Period of time before WISP requests time out (1 - 15 sec, default = 5). range
[1-15]
    next
end
```

Example configuration

```
    config web-proxy wisp
       edit 0
          set outgoing-ip 0.0.0.0
          set server-ip 0.0.0.0
          set server-port 15868
```

```
      set max-connections 64
      set timeout 5
   next
end
```

After configuring the WISP server, enable WISP in the web filter profile.

```
config webfilter profile
   edit "wisp_only"
      set wisp enable
      set wisp-servers 0
   next
end
```

Now you can apply the web filter profile to a firewall policy.

If you configure more than one WISP server, the load balance option can also be configured.

```
config webfilter profile
   edit "wisp_only"
      set wisp-algorithm {primary-secondary | round-robin | auto-learning}
   next
end
```

The options for the `wisp-algorithm` are:

- `primary-secondary`: select the first healthy server in order
- `round-robin`: select the next healthy server
- `auto-learning` select the lightest loading healthy server

DNS filter

You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiGate must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

If that FortiGuard category is set to **block**, the result of the DNS lookup is not returned to the requester. If the category is set to **redirect**, then the address returned to the requester points at a FortiGuard redirect page.

You can also allow or monitor access based on FortiGuard category.

Blocking DNS requests to known botnet command & control addresses

FortiGuard maintains a database containing a list of known botnet command and control (C&C) addresses. This database is updated dynamically and stored on the FortiGate and requires a valid FortiGuard AntiVirus subscription.

When you block DNS requests to known botnet C&C addresses, using IPS, DNS lookups are checked against the botnet C&C database. All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all sub-domains are also blocked.

To enable this feature, go to **Security Profiles > DNS Filter**, and enable **Block DNS requests to known botnet C&C**.

Static Domain Filter

The DNS **Static Domain Filter** allows you to block, exempt, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match the DNS request can be blocked, exempted, monitored, or allowed.

If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site.

If exempted, access to the site is allowed even if another method is used to block it.

CLI commands

- Rename `webfilter-sdns-server-ip` and `webfilter-sdns-server-port`:

```
config system fortiguard
   set sdns-server-ip x.x.x.x
   set sdns-server-port 53
end
```

- Configure DNS domain filter lists in order to decide access for specific domains:

```
config dnsfilter domain-filter
   edit {id}
      set id {integer}
      set name {string}
      set comment {string}
      config entries
         edit {id}
```

```
        set id {integer}
        set domain {string}
        set type {simple | regex | wildcard}
        set action {block | allow | monitor}
        set status {enable | disable}
      next
   next
end
```

- Configure DNS filter profile:

```
config dnsfilter profile
   edit "dns_profile1"
      set comment ''
         config domain-filter
            set domain-filter-table <id>
            set external-blocklist [addr1] [addr2] [addr3]
         end
         config ftgd-dns
              config filters
                 edit 1
                    set category 49
                    set action block
                    set log enable
                 next
                 edit 2
                    set category 71
                    set action monitor
                    set log enable
                 next
              end
         end
      set log-all-url disable
      set block-action redirect
      set redirect-portal 0.0.0.0
      set block-botnet enable
   next
end
```

- Configure DNS profile in a firewall policy:

```
config firewall policy
   edit 1
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "FTP"
      set utm-status enable
      set dnsfilter-profile "dns_profile1"
      set profile-protocol-options "default"
      set nat enable
   next
end
```

- Configure DNS profile in profile group:

```
config firewall profile-group
   edit "pgrp1"
      set dnsfilter-profile "dns_profile1"
      set profile-protocol-options "default"
   next
end
```

DNS profile supports safe search

Users can take advantage of pre-defined DNS filter rules to edit DNS profiles and provide safe search for Google, Bing, and YouTube.

To add safe search to a DNS profile - GUI

1. Go to **Security Profiles > DNS Filter**.
2. Edit the default filter or create a new one.
3. Enable **Enforce 'Safe Search' on Google, Bing, YouTube**.
4. Select **Strict** or **Moderate** level for **Restrict YouTube Access**.

To add safe search to a DNS profile - CLI

```
config dnsfilter profile
   edit "default"
      set safe-search enable
      set youtube-restrict {strict | moderate} (only available if safe-search enabled)
   next
end
```

FortiGuard botnet protection

Preventing botnets from controlling your system is achieved by detecting and blocking connection attempts to known botnets. This feature also blocks connections to known phishing sites. The FortiGuard database is continually updated with addresses of known Command and Control (C&C) sites that botnet clients attempt to connect to, as well as a addresses of known phishing URLs.

To enable botnet and phishing protection in a DNS Filter profile, enable **Block DNS requests to known botnet C&C**.

The latest botnet database is available from FortiGuard. To see the version of the database and display its contents, go to **System > FortiGuard > AntiVirus** and view the lists for **Botnet IPs** and **Botnet Domains**. You can look up more details about Botnet IPs and Domains on the FortiGuard site.

You can block, monitor, or allow outgoing connections to botnet sites for each FortiGate interface.

The DNS Filter security profile and the botnet protection features are available for both proxy-based and flow-based inspection modes.

Application control

Using the Application Control Security Profiles feature, your FortiGate unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols. Application control supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).

The FortiGate unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

Fortinet is constantly adding to the list of applications detected through maintenance of the FortiGuard Application Control Database. This database is part of the FortiGuard Intrusion Protection System Database because intrusion protection protocol decoders are used for application control and both of these databases have the same version number.

Cloud Access Security Inspection (CASI) is merged with Application Control resulting in changes to the GUI and the CLI.

You can identify the version of the application control database installed on your unit by going to the **Licenses** widget on the **Dashboard** and hovering over the **IPS & Application Control** line; the status, expiry date, and version will be displayed. Additionally, you can see the complete list of applications supported by FortiGuard Application Control on the FortiGuard site or http://fortiguard.com/appcontrol. This web page lists all of the supported applications. You can select any application name to see details about the application.

Application Control is a standard part of any FortiCare support contract and the database for Application Control signatures is separate from the IPS database. However, botnet application signatures are still part of the IPS signature database since these are more closely related with security issues and less about application detection.

This Handbook chapter includes Inside FortiOS: Application Control and provides readers an overview of the features and benefits of key FortiOS 5.6 components. For readers needing to delve into greater detail, we provide the following topics:

Application control concepts

You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 2,000 applications, services, and protocols.

Updated and new application signatures are delivered to your FortiGate unit as part of your FortiGuard Application Control Service subscription, which is a free service. Fortinet is constantly increasing the number of applications that this feature can detect by adding applications to the FortiGuard Application Control Database. Because intrusion protection protocol decoders are used for application control, the application control database is part of the FortiGuard Intrusion Protection System Database. Both of these databases have the same version number.

You can find the version of the application control database installed on your unit by going to the **Licenses** widget on the **Dashboard** and hovering over the **IPS& Application Control** line; the status, expiry date, and version will be displayed.

To see the complete list of applications supported by FortiGuard Application Control go to the FortiGuard site or http://fortiguard.com/appcontrol. This web page lists all of the supported applications. You can select any application name to see details about the application.

Enabling application control in profile-based modes

Application control examines your network traffic for traffic generated by the applications you want it to control. The configuration steps outlined below are for FortiGate's operating in proxy-based inspection and flow-based inspection with profile-based NGFW modes. For FortiGate's operating in NGFW policy-based mode, see Enabling application control in NGFW policy-based mode.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an application sensor.
2. Configure the sensor to include the signatures for the application traffic you want the FortiGate unit to detect.
3. Enable any other applicable options.
4. Enable application control in a security policy and select the application sensor.

Creating an application sensor

You need to create an application sensor before you can enable application control.

To create an application sensor

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter the name of the new application sensor.
4. Optionally, enter descriptive **Comments**.

Adding applications to an application sensor

Once you have created an application sensor, you need to need to define the applications that you want to control. You can add applications and filters using categories, application overrides, and/or filter overrides. Categories will allow you to choose groups of signatures based on a category type. Application overrides allow you to choose individual applications. Filter overrides allow you to select groups of applications and override the application signature settings for them.

To add a category of signatures to the sensor.

1. Go to **Security Profiles > Application Control**.
2. Under **Categories**, you may select from the following:
   - Business
   - Cloud,.IT
   - Collaboration
   - Email
   - Game
   - General.Interest
   - Industrial
   - Mobile
   - Network.Service
   - P2P
   - Proxy
   - Remote.Access
   - Social.Media
   - Storage.Backup
   - Update
   - Video/Audio
   - VoIP
   - Web.Client
   - Unknown Applications

   When selecting the category that you intend to work with, left click on the icon next to the category name to see a drop down menu that includes these actions:

   - Allow
   - Monitor
   - Block
   - Quarantine
   - View Signatures

These actions are briefly defined under Application control actions on page 128.

3. If you wish to add individual applications, select **Add Signatures** under **Application Overrides**.
   a. Use the **Add Filter** search field to narrow down the list of possible signatures by a series of attributes.
   b. When finished, select **Use Selected Signatures**.
4. If you wish to add advanced filters, select **Add Filter** under **Filter Overrides**.
   a. Use the Add Filter search field to narrow down the list of possible filters by a series of attributes.
   b. When finished, select **Use Filters**.
4. Select, if applicable, from the following options:
   - **Allow and Log DNS Traffic**
   - **Replacement Messages for HTTP-based Applications**
6. Select **OK**.

Applying the application sensor to a security policy

An application sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an application sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the application sensor in a security policy — GUI

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select a policy.
3. Click the **Edit** icon.
4. Under the heading **Security Profiles** toggle the button next to **Application Control** to enable the feature.
5. In the drop down menu field next to the **Application Control** select the application sensor you wish to apply to the policy.
6. Select **OK**.

Creating a new custom application signature

If you have to deal with an application that is not already in the **Application List** you have the option to create a new application signature.

1. Go to **Security Profiles > Application Control**.
2. Select the link in the upper right corner, **[View Application Signatures]**
3. Select the **Create New** icon
4. Give the new signature a name (no spaces) in the **Name** field.
5. Enter a brief description in the **Comments** field
6. Enter the text for the signature in the signature field. Use the rules found under Custom IPS signature to determine syntax.
7. Select **OK.**

You can configure rate based application control signatures in the CLI Console using similar IPS signature rate CLI commands.

For more information on this and the CLI syntax, see IPS signature rate count threshold on page 145

Messages in response to blocked applications

Once an Application Control sensor has been configured to block a specified application and applied to a policy it would seem inevitable that at some point an application will end up getting blocked, even if it is only to test the functionality of the control. When this happens, the sensor can be set to either display a message to offending user or to just block without any notification. The default setting is to display a message. Setting this up is done in the CLI.

```
config application list
   edit <name of the sensor>
      set app-replacemsg {enable | disable}
   end
```

When blocking applications, there is no replacement message for SSL traffic with certificate inspection applied.
When SSL deep inspection is enabled, a replacement message will appear depending on the protocol. For example, with HTTP2, the blocking is done in the SSL key exchange once the first server packet is delivered and replacement messages can not be displayed.

P2P application detection

P2P software tends to be evasive. You may be able to enhance P2P application detection by matching patterns found in the most recent three minutes of P2P traffic to determine if new traffic is P2P. Three minutes is the length of time information about matched P2P traffic remains in shared memory.

For example, the CLI commands below will result in the Intrusion Prevention System (IPS) looking for patterns formed by Skype traffic.

```
config application list
   edit <app_list_str>
      set p2p-black-list skype
   end
end
```

Application control actions

Allow

This action allows the targeted traffic to continue on through the FortiGate unit.

Monitor

This action allows the targeted traffic to continue on through the FortiGate unit but logs the traffic for analysis.

Block

This action prevents all traffic from reaching the application and logs all occurrences.

Quarantine

This action allows you to quarantine or block access to an application for a specified duration that can be entered in days, hours, and minutes. The default is 5 minutes.

View Signatures

This option brings up a window that displays a list of the signatures with the following columns:

- Name
- Category
- Technology - Technology is broken down into 3 technology models as well as the more basic Network-Protocol which would can be used as a catch all for anything not covered by the more narrowly defined technologies of:
  - Browser-Based
  - Client-Server
  - Peer-to-Peer
- Popularity - Popularity is broken down into 5 levels of popularity represented by stars.
- Risk - The Risk property does not indicate the level of risk but the type of impact that is likely to occur by allowing the traffic from that application to occur.

Traffic Shaping

Prior to the release of FortiOS 5.4.0, application control traffic shaping was configured in the **Security Profiles > Application Control** interface. There is now a specific section for traffic shaping policies in **Policy & Objects > Traffic Shaping Policy**. See Traffic shaping methods in the chapter on Traffic Shaping for details

Application considerations

Some applications behave differently from most others. You should be aware of these differences before using application control to regulate their use.

IM applications

IM applications are controlled by either permitting or denying the users from logging in to the service. Individual IM accounts are configured as to whether or not they are permitted and then there is a global policy for how to action unknown users, by the application and whether to add the user to the black list or the white list. IM applications fall under the **Collaboration** category in the application signature database.

Skype

Based on the NAT firewall type, Skype takes advantage of several NAT firewall traversal methods, such as STUN (Simple Traversal of UDP through NAT), ICE (Interactive Connectivity Establishment) and TURN (Traversal Using Relay NAT), to make the connection.

The Skype client may try to log in with either UDP or TCP, on different ports, especially well-known service ports, such as HTTP (80) and HTTPS (443), because these ports are normally allowed in firewall settings. A client who has previously logged in successfully could start with the known good approach, then fall back on another approach if the known one fails.

The Skype client could also employ Connection Relay. This means if a reachable host is already connected to the Skype network, other clients can connect through this host. This makes any connected host not only a client but also a relay server.

SPDY

SPDY (pronounced speedy, it's a trademarked name not an acronym) is a networking protocol developed to increase the speed and security of HTML traffic. It was developed primarily by Google. The Application Control engine recognizes this protocol and its required SSL/TLS component within Application Control sensors. It is counted as part of application traffic for Google and other sources that use the protocol.

Application control monitor

The application monitor enables you to gain insight into the applications generating traffic on your network. When monitor is enabled in an application sensor entry and that security profile is selected in a security policy, all the detected traffic required to populate the selected charts is logged to the SQL database on the FortiGate unit hard drive. The charts are available for display in the **Applications** section of the **FortiView** menu.

Because the application monitor relies on an SQL database, the feature is available only on FortiGate units with an internal hard drive.

Application monitor data is stored on the hard drive and restarting the system does not affect the stored monitor data.

Application control data is available in **Log & Report**, if enabled.

Application control examples

The scenarios below provide a better understanding of how to implement Application Control and give some ideas as to why it would be used.

- Blocking instant messaging
- Allowing only software updates
- Blocking Windows XP with a custom signature

Blocking instant messaging

Instant messaging use is not permitted at the Example Corporation. Application control helps enforce this policy.

The configuration steps outlined below are for FortiGate's operating in proxy-based inspection and flow-based inspection with profile-based NGFW modes. For FortiGate's operating in NGFW policy-based mode, see Enabling application control in NGFW policy-based mode.

Steps in this process

1. First you will create an application sensor with a single entry that monitors the category that includes instant messaging applications. You will set the list action to **Monitor**.
2. Next you will assign the sensor to a policy.
3. Then you will identify the IM applications being used on your network and modify the application sensor to **Block** use of those messaging applications

To create the application sensor

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter `no_IM` for the application sensor name.
4. If the **Collaboration** category is not already set to **Monitor**, then left-click on the icon next to that category and select **Monitor** from the dropdown menu.
5. Select **OK** to save the new sensor.

To enable application control and select the application sensor

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select the security policy that allows the network users to access the Internet and choose **Edit**.
3. Under the heading **Security Profiles** toggle the button next to **Application Control** to turn it on.
4. In the drop down menu field next to the **Application Control** select the **no_IM** application sensor.
5. To inspect all traffic, **SSL/SSH inspection** must be set to **deep-inspection** profile.
6. Select **OK**.

To identify IM applications in use on your network

1. Go to **FortiView > Applications**.
2. Select a time period from the options in the upper-right corner of the window and examine the list of applications.
3. Identify any IM applications you wish to block.

To block IM applications in use on your network

1. Go to **Security Profiles > Application Control** and edit the **no_IM** application sensor.
2. Under **Application Overrides**, click on **Add Signatures**.
3. Filter by **Name** and select the IM applications you wish to block.
4. Click on **Use Selected Signatures**.

The selected application will appear under Application Overrides and the action will be set to Block.

5. Select **Apply**.

The IM applications identified will be blocked by the security policy that has the **no IM** application sensor applied to it. If other firewall policies handle traffic that users could use for applications in the same category, enable application control with the **no IM** application sensor for those policies as well.

Allowing only software updates

Some departments at Example Corporation do not require access to the Internet to perform their duties. Management therefore decided to block their Internet access. Software updates quickly became an issue because automatic updates will not function without Internet access and manual application of updates is time-consuming.

The solution is configuring application control to allow only automatic software updates to access the Internet.

The configuration steps outlined below are for FortiGate's operating in proxy-based inspection and flow-based inspection with profile-based NGFW modes. For FortiGate's operating in NGFW policy-based mode, see Enabling application control in NGFW policy-based mode.

To create an application sensor — GUI

1. Go to **Security Profiles > Application Control**.
2. Select the **Create New** icon in the title bar of the **Edit Application Sensor** window.
3. In the **Name** field, enter `Updates_Only` as the application sensor name.
4. Using the left-click and drop down on the items in the **Category** list.
   a. Select **Monitor** from the dropdown menu.
   b. Select **Block** for the rest of the categories.
5. Select **OK**.

To create an application sensor — CLI

```
config application list
   edit Updates_Only
      config entries
         edit 1
            set category 17
            set action pass
         end
      set other-application-action block
      set unknown-application-action block
   end
```

You will notice that there are some differences in the naming convention between the GUI and the CLI. For instance the **Action** in the CLI is "`pass`" and the **Action** in the GUI is "**Monitor**".

Selecting the application sensor in a security policy

An application sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an application sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the application sensor in a security policy — GUI

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select a policy.
3. Select the **Edit** icon.
4. Under the heading **Security Profiles** toggle the button next to **Application Control** to turn it on.
5. In the drop down menu field next to the **Application Control** select the `Updates_only` list.
6. Select **OK**.

To select the application sensor in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set profile-protocol-options default
      set application-list Updates_Only
   end
```

Traffic handled by the security policy you modified will be scanned for application traffic. Software updates are permitted and all other application traffic is blocked.

Blocking Windows XP with a custom signature

In this example, you will use application control to block web traffic from PCs running Windows operating systems NT 5, including Windows XP and Windows Server 2003 (includes Windows virtual machines).

When a computer's operating system lacks vendor support, it becomes a threat to the network because newly discovered exploits will not be patched. Using the FortiGate application control feature, you can restrict these computers from accessing external resources.

This example will only block web traffic from computers running the affected operating systems. If you wish to block these computers from being on the network entirely, further action will be necessary. However, the logs generated can be used to identify the computers you wish to block.

1. Go to **System > Feature Select**. Enable **Application Control** and **Apply** your changes.
2. Go to **Security Profiles > Application Control** and select **View Application Signatures**.
3. Create a new signature with the syntax below. You can copy and paste the text into the **Signature** field. Name the signature *Block-Windows-NT5*.

   ```
   F-SBID(--attack_id 8055;--vuln_id 8055;--name
   "Windows.NT.5.Web.Surfing";--flow from_client;--pattern !"FCT";--
   pattern "Windows NT 5.";--no_case;--context header;--weight 40;--
   service HTTP;--protocol tcp;--app_cat 25;--default_action drop_
   session;)
   ```

   If you do not include keyword / value pairs for `--attack_id` or `--vuln_ID` in the signature, the FortiGate will automatically assign values.

   The signature will appear at the top of the application list and be listed in the **Web.Client** category.
4. Go to **Security Profiles > Application Control** and edit the **default** policy.
5. Under **Application Overrides**, select **Add Signatures**. The new signature should appear at the top of the list. If it does not, search for the signature's name.
6. Select the signature, then select **Use Selected Signatures**.

7. Go to **Policy & Objects > IPv4 Policy** and edit the policy that allows connections from the internal network to the Internet.
8. Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Results

When a PC running one of the affected operating systems attempts to connect to the Internet using a browser, a blocked message appears. Because Application Control uses flow-based inspection, if you apply an additional security profile to your traffic that is proxy-based, the connection will simply timeout rather than display the replacement message. However, Application Control will still function.

PCs running other operating systems, including later versions of Windows, are not affected.

Go to **FortiView > All Sessions** and select the **5 minutes** view.

Filter the results to show sessions that were blocked.

You will see that the Application Control signature, shown in the **Application Name** column, was used to block traffic from PCs running older Windows versions.

For further reading, see Custom Application & IPS Signatures.

Intrusion prevention

The FortiOS Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

This section describes how to configure the FortiOS Intrusion Prevention settings.

This Handbook chapter includes Inside FortiOS: Intrusion Prevention System providing readers an overview of the features and benefits of key FortiOS 5.6 components. For readers needing to delve into greater detail, we provide the following:

IPS concepts

The FortiOS Intrusion Prevention System (IPS) protects your network from outside attacks. Your FortiGate unit has two techniques to deal with these attacks: anomaly- and signature-based defense.

Anomaly-based defense

Anomaly-based defense is used when network traffic itself is used as a weapon. A host can be flooded with far more traffic than it can handle, making the host inaccessible. The most common example is the denial of service (DoS) attack, in which an attacker directs a large number of computers to attempt normal access of the target system. If enough access attempts are made, the target is overwhelmed and unable to service genuine users. The attacker does not gain access to the target system, but it is not accessible to anyone else.

The FortiGate DoS feature will block traffic above a certain threshold from the attacker and allow connections from other legitimate users. The DoS policy configuration can be found in the Firewall chapter of the Handbook.

Access control lists in DoS Policies

This feature allows you to define a list of IPs/subnets/ranges in a DoS policy, and block those IPs from sending any traffic, by way of an ACL (access control list). The ACL looks similar to a firewall policy, but only checks source IP, destination IP, destination port, and protocol. To configure in the GUI, go to **Policy & Objects > IPv4 Access Control List** and create a new policy. Enter the incoming interface, the source address, the destination address, the services impacted, and, optionally, enter a comment.

CLI Syntax

```
config firewall acl
   edit 1
```

```
        set interface "port1"
        set srcaddr "google-drive"
        set dstaddr "all"
        set service "ALL"
    next
end
```

Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access and this communication will include particular commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiGate unit to detect and stop the attack.

Signatures

IPS signatures are the basis of signature-based intrusion prevention. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information so your FortiGate unit knows what to look for in network traffic.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol in which the attack will appear, the vulnerable operating system, and the vulnerable application.

To view the complete list of signatures, go to **Security Profiles > Intrusion Prevention**, and select **View IPS Signatures**. This will include the predefined signatures and any custom signatures that you may have created.

With the release of FortiOS 5.6, the IPS signatures list page shows which IPS package is currently deployed. Users can also change their IPS package by hovering over the information icon next to the IPS package name. Text will appear that links directly to the FortiGate's **System > FortiGuard** page from the IPS Signatures list page.

Protocol decoders

Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiGate unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiGate unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.

IPS engine

Once the protocol decoders separate the network traffic by protocol, the IPS engine examines the network traffic for the attack signatures.

IPS sensors

The IPS engine does not examine network traffic for all signatures. You must first create an IPS sensor and specify which signatures are included. Add signatures to sensors individually using signature entries, or in groups using IPS filters.

To view the IPS sensors, go to **Security Profiles > Intrusion Prevention**.

You can group signatures into IPS sensors for easy selection when applying to firewall policies. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic. For example, you can specify all of the web-server related signatures in an IPS

sensor, and that sensor can then be applied to a firewall policy that controls all of the traffic to and from a web server protected by the unit.

The FortiGuard Service periodically updates the pre-defined signatures, with signatures added to counter new threats. Since the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Each IPS sensor consists of two parts: filters and overrides. Overrides are always checked before filters.

Each filter consists of a number of signatures attributes. All of the signatures with those attributes, and only those attributes, are checked against traffic when the filter is run. If multiple filters are defined in an IPS Sensor, they are checked against the traffic one at a time, from top to bottom. If a match is found, the unit takes the appropriate action and stops further checking.

A signature override can modify the behavior of a signature specified in a filter. A signature override can also add a signature not specified in the sensor's filters. Custom signatures are included in an IPS sensor using overrides.

The signatures in the overrides are first compared to network traffic. If the IPS sensor does not find any matches, it then compares the signatures in each filter to network traffic, one filter at a time, from top to bottom. If no signature matches are found, the IPS sensor allows the network traffic.

The signatures included in the filter are only those matching every attribute specified. When created, a new filter has every attribute set to **all** which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

IPS filters

IPS sensors contain one or more IPS filters. A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS filter.

For example, if your FortiGate unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting **OS** to **Linux**, and **Application** to **Apache,** the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS sensor, go to **Security Profiles > Intrusion Prevention**, select the IPS sensor containing the filters you want to view, and select **Edit**.

Custom/predefined signature entries

Signature entries allow you to add an individual custom or predefined IPS signature. If you need only one signature, adding a signature entry to an IPS sensor is the easiest way. Signature entries are also the only way to include custom signatures in an IPS sensor.

Another use for signature entries is to change the settings of individual signatures that are already included in a filter within the same IPS sensor. Add a signature entry with the required settings above the filter, and the signature entry will take priority.

Policies

To use an IPS sensor, you must select it in a security policy or an interface policy. An IPS sensor that it not selected in a policy will have no effect on network traffic.

IPS is most often configured as part of a security policy. Unless stated otherwise, discussion of IPS sensor use will be in regards to firewall policies in this document.

Session timers for IPS sessions

A session time-to-live (TTL) timer for IPS sessions is available to reduce synchronization problems between the FortiOS Kernel and IPS, and to reduce IPS memory usage. The timeout values can be customized.

Enabling IPS scanning

Enabling IPS scanning involves two separate features of FortiOS 5.6:

- The security policy allows certain network traffic based on the sender, receiver, interface, traffic type, and time of day. Firewall policies can also be used to deny traffic, but those policies do not apply to IPS scanning.
- The IPS sensor contains filters, signature entries, or both. These specify which signatures are included in the IPS sensor.

When IPS is enabled and an IPS sensor is selected in a security policy, and all network traffic matching the policy will be checked for the signatures in the IPS sensor.

General configuration steps

For best results in configuring IPS scanning, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an IPS sensor.
2. Add signatures and /or filters.
   These can be:
   - Pattern based
   - Rate based
   - Customized
3. Select a security policy or create a new one.
4. In the security policy, turn on **IPS**, and choose the IPS sensor from the list.

All the network traffic controlled by this security policy will be processed according to the settings in the policy. These settings include the IPS sensor you specify in the policy.

Creating an IPS sensor

You need to create an IPS sensor before specific signatures or filters can be chosen. The signatures can be added to a new sensor before it is saved. However, it is good practice to keep in mind that the sensor and its included filters are separate things, and that they are created separately.

To create a new IPS sensor

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select the **Create New** icon in the top of the Edit IPS Sensor window.
3. Enter the name of the new IPS sensor.

4. Optionally, enter a comment. The comment will appear in the IPS sensor list.
5. Select **OK**.

A newly created sensor is empty and contains no filters or signatures. You need to add one or more filters or signatures before the sensor will be of any use.

Adding an IPS filter to a sensor

While individual signatures can be added to a sensor, a filter allows you to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added.

To create a new pattern based signature and filter

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select the IPS sensor to which you want to add the filter using the drop-down list in the top row of the Edit IPS Sensor window or by going to the list window.
3. Under **IPS Filters**, select **Add Filter**.
4. Configure the filter that you require. Signatures matching all of the characteristics you specify in the filter will be included in the filter. Once finished, select **Use Filters**.

Application refers to the application affected by the attack and filter options include over 25 applications.

OS refers to the Operating System affected by the attack. The options include **BSD**, **Linux**, **MacOS**, **Other**, **Solaris**, and **Windows**.

Protocol refers to the protocol that is the vector for the attack; filter options include over 35 protocols, including "other."

Severity refers to the level of threat posed by the attack. The options include **Critical**, **High**, **Medium**, **Low**, and **Info**.

Target refers to the type of device targeted by the attack. The options include **client** and **server**.

5. Once you have selected the filters you wish to add, right-click the filters and choose an action for when a signature is triggered:

Action	Description
Pass	Select **Pass** to allow traffic to continue to its destination. **Note:** to see what the default for a signature is, go to the **IPS Signatures** page and enable the column **Action**, then find the row with the signature name in it.
Monitor	Select **Monitor** to allow traffic to continue to its destination and log the activity. The log will appear under Log & Report but will only be visible in the GUI in the event of an intrusion.
Block	Select **Block** to drop traffic matching any the signatures included in the filter.
Reset	Select **Reset** to reset the session whenever the signature is triggered. In the CLI this action is referred to as Reject.

Action	Description
Default	Select **Default** to use the default action of the signature.
Quarantine	The quarantine based on the attacker's IP Address - Traffic from the Attacker's IP address is refused until the expiration time from the trigger is reached. You may set the **Quarantine Duration** to any number of **Days**, **Hours**, or **Minutes**.
Packet Logging	Select to enable packet logging for the filter. When you enable packet logging on a filter, the unit saves a copy of the packets that match any signatures included in the filter. The packets can be analyzed later. For more information about packet filtering, see "Configuring packet logging options".

6. Select **Apply**.

The filter is created and added to the filter list.

Adding rate based signatures

These are a subset of the signatures that are found in the database that are normally set to monitor. This group of signatures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, a little like DoS attacks.

Adding a rate based signature is straight forward. Select the enable button in the Rate Based Signature table that corresponds with the desired signature.

Customized signatures

Customized signatures must be created before they can be added to the sensor. To get more details on customized signatures check the Custom Application & IPS Signatures chapter.

Updating predefined IPS signatures

The FortiGuard Service periodically updates the predefined signatures and adds new signatures to counter emerging threats as they appear.

To ensure that your system is providing the most protection available, these updates can be scheduled as often as on an hourly basis. To configure this feature, go to **System > FortiGuard**. Under **AntiVirus & IPS Updates**, enable **Scheduled Updates**. From here you can set the updates to occur on a consistent weekly, daily, or even hourly basis.

Because the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Viewing and searching predefined IPS signatures

Go to **Security Profiles > Intrusion Prevention**. Select **[View IPS Signatures]** to view the list of existing IPS signatures. You may find signatures by paging manually through the list, apply filters, or by using the search field.

Searching manually

Signatures are displayed in a paged list, with 50 signatures per page. The bottom of the screen shows the current page and the total number of pages. You can enter a page number and press enter, to skip directly to that page. Previous Page and Next Page buttons move you through the list, one page at a time. The First Page and Last Page button take you to the beginning or end of the list.

Searching CVE-IDs

A **CVE-ID** column displaying CVE-IDs can be optionally added to the IPS Signatures list, however the column is only available if the IPS package contains CVE-IDs for signatures. CVE-IDs can be numerically filtered by selecting the CVE-ID column's arrows.

Applying filters

You can enter criteria for one of more columns, and only the signatures matching all the conditions you specify will be listed.

To apply filters

1. Go to **Security Profiles > Intrusion Prevention.** Select **[View IPS Signatures] .**
2. Select column by which to filter.
3. Select the funnel/filter icon and enter the value or values to filter by.
4. Use additional columns as needed to refine search.

The available options vary by column. For example, **Enable** allows you to choose between two options, while OS has multiple options, and you may select multiple items together. Filtering by name allows you to enter a text string and all signature names containing the string will be displayed.

IPS processing in an HA cluster

IPS processing in an HA cluster is no different than with a single FortiGate unit, from the point of view of the network user. The difference appears when a secondary unit takes over from the primary, and what happens depends on the HA mode.

Active-passive

In an active-passive HA cluster, the primary unit processes all traffic just as it would in a stand-alone configuration. Should the primary unit fail, a secondary unit will assume the role of the primary unit and begin to process network traffic. By default, the state of active communication sessions are not shared with secondary units and will not survive the fail-over condition. Once the sessions are reestablished however, traffic processing will continue as normal.

If your network requires that active sessions are taken over by the new primary unit, select **Enable Session Pick-up** in your HA configuration. Because session information must be sent to all subordinate units on a regular basis, session pick-up is a resource-intensive feature and is not enabled by default.

Active-active

The fail-over process in an active-active cluster is similar to an active-passive cluster. When the primary unit fails, a secondary unit takes over and traffic processing continues. The load-balancing schedule used to distribute sessions to the cluster members is used by the new primary unit to redistribute sessions among the remaining subordinate units. If session pick-up is not enabled, the sessions active on the failed primary are lost, and the sessions redistributed among the secondary units may also be lost. If session pick-up is enabled, all sessions are handled according to their last-known state.

Configure IPS options

The following IPS configuration options are available:

- Malicious URL database for drive-by exploits detection
- Customizable replacement message when IPS blocks traffic
- Hardware acceleration
- Extended IPS database
- Configuring the IPS engine algorithm
- Configuring the IPS engine-count
- Configuring fail-open
- Configuring the session count accuracy
- Configuring IPS intelligence
- Configuring the IPS buffer size
- Configuring protocol decoders
- Configuring security processing modules
- IPS signature rate count threshold
- Geographic location filter

Malicious URL database for drive-by exploits detection

This feature uses a local malicious URL database on the FortiGate to assist in drive-by exploits detection. The database contains all malicious URLs active in the last one month, and all drive-by exploit URLs active in the last three months. The number of URLs controlled are in the one million range.

```
config ips sensor
   edit <profile>
      set block-malicious-url [enable | disable]
   next
end
```

Customizable replacement message when IPS blocks traffic

You can edit a replacement message that will appear specifically for IPS sensor blocked Internet access. Go to **System > Replacement Messages**, select **Extended View** and find **IPS Sensor Block Page** under the **Security** heading.

Hardware acceleration for flow-based security profiles (NTurbo and IPSA)

Some FortiGate models support a feature call NTurbo that can offload flow-based firewall sessions to NP4 or NP6 network processors. Some FortiGate models also support offloading enhanced pattern matching for flow-based security profiles to CP8 or CP9 content processors. You can use the following command to configure NTurbo and IPSA:

```
config ips global
   set np-accel-mode {none | basic}
   set cp-accel-mode {none | basic | advanced}
end
```

If the `np-accel-mode` option is available, your FortiGate supports NTurbo: `none` disables NTurbo and `basic` (the default) enables NTurbo. If the `cp-accel-mode` option is available your FortiGate supports IPSA: `none` disables IPSA, `basic` enables basic IPSA and `advanced` enables enhanced IPSA which can offload more types of pattern matching than basic IPSA. `advanced` is only available on FortiGate models with two or more CP8 processors or one or more CP9 processors.

See the **Hardware Acceleration** handbook chapter for more information about NTurbo and IPSA.

Extended IPS database

Some models have access to an extended IPS Database. The extended database may affect the performance of the FortiGate unit so depending on the model of the FortiGate unit the extended database package may not be enabled by default. For example, the D-series Desktop model have this option disabled by default.

This feature can only be enbled through the CLI.

```
config ips global
   set database extended
end
```

Configuring the IPS engine algorithm

The IPS engine is able to search for signature matches in two ways. One method is faster but uses more memory, the other uses less memory but is slower. Use the `algorithm` CLI command to select one method:

```
config ips global
   set algorithm {super | high | low | engine-pick}
end
```

Specify `high` to use the faster more memory intensive method or `low` for the slower memory efficient method. The setting `super` improves the performance for FortiGate units with more than 4GB of memory. The default setting is `engine-pick`, which allows the IPS engine to choose the best method on the fly.

Configuring the IPS engine-count

FortiGate units with multiple processors can run more than one IPS engine concurrently. The `engine-count` CLI command allows you to specify how many IPS engines are used at the same time:

```
config ips global
   set engine-count <int>
end
```

The recommended and default setting is `0`, which allows the FortiGate unit to determine the optimum number of IPS engines.

Configuring fail-open

IPS is likely more important to your network than uninterrupted flow of network traffic, so the fail-open behaviour of the IPS engine is disabled by default. If you would like to enable the fail-open option, use the following syntax. When enabled, if the IPS engine fails for any reason, it will fail open. This applies for inspection of all the protocols inspected by FortiOS IPS protocol decoders, including but not limited to HTTP, HTTPS, FTP, SMTP, POP3, IMAP, etc. This means that traffic continues to flow without IPS scanning. To enable:

```
config ips global
   set fail-open {enable | disable}
end
```

The default setting is `disable`.

Configuring the session count accuracy

The IPS engine can keep track of the number of open session in two ways. An accurate count uses more resources than a less accurate heuristic count.

```
config ips global
   set session-limit-mode {accurate | heuristic}
end
```

The default is `heuristic`.

Configuring IPS intelligence

Starting with FortiOS 5.2, `intelligent-mode` is a new adaptive detection method. This command is enabled the default and it means that the IPS engine will perform adaptive scanning so that, for some traffic, the FortiGate can quickly finish scanning and offload the traffic to NPU or kernel. It is a balanced method which could cover all known exploits. When disabled, the IPS engine scans every single byte.

```
config ips global
   set intelligent-mode {enable|disable}
end
```

Configuring the IPS buffer size

Set the size of the IPS buffer.

```
config ips global
   set socket-size <int>
end
```

The acceptable range is from 1 to 64 megabytes. The default size varies by model. In short, `socket-size` determines how much data the kernel passes to the IPS engine each time the engine samples packets.

Configuring protocol decoders

The FortiGate Intrusion Prevention system uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

To change the ports a decoder examines, you must use the CLI. In this example, the ports examined by the DNS decoder are changed from the default 53 to 100, 200, and 300.

```
config ips decoder dns_decoder
   set port_list "100,200,300"
end
```

You cannot assign specific ports to decoders that are set to **auto** by default. These decoders can detect their traffic on any port. Specifying individual ports is not necessary.

Configuring security processing modules

FortiGate Security Processing Modules, such as the CE4, XE2, and FE8, can increase overall system performance by accelerating some security and networking processing on the interfaces they provide. They also allow the FortiGate unit to offload the processing to the security module, thereby freeing up its own processor for other tasks. The security module performs its own IPS and firewall processing, but you can configure it to favor IPS in hostile high-traffic environments.

If you have a security processing module, use the following CLI commands to configure it to devote more resources to IPS than firewall. This example shows the CLI commands required to configure a security module in slot 1 for increased IPS performance.

```
config system amc-slot
   edit sw1
      set optimization-mode fw-ips
      set ips-weight balanced
      set ips-p2p disable
      set ips-fail-open enable
      set fp-disable none
      set ipsec-inb-optimization enable
      set syn-proxy-client-timer 3
      set syn-proxy-server-timer 3
   end
```

In addition to offloading IPS processing, security processing modules provide a hardware accelerated SYN proxy to defend against SYN flood denial of service attacks. When using a security module, configure your DoS anomaly check for `tcp_syn_flood` with the **Proxy** action. The **Proxy** action activates the hardware accelerated SYN proxy.

IPS signature rate count threshold

The IPS signature threshold can allow configuring a signature so that it will not be triggered until a rate count threshold is met. This provides a more controlled recording of attack activity. For example, if multiple login attempts produce a failed result over a short period of time then an alert would be sent and perhaps traffic blocked. This would be a more rational response than sending an alert every time a login failed.

The syntax for this configuration is as follows:

```
config ips sensor
   edit default
      config entries
         edit <Filter ID number>
            set rule <*id>
            set rate-count <integer between 1 - 65535>
            set rate-duration <integer between 1 - 65535>
```

The value of the rate-duration is an integer for the time in seconds.

```
set rate-mode <continuous | periodical>
```

The rate-mode refers to how the count threshold is met.

If the setting is "`continuous`", and the action is set to block, as soon as the `rate-count` is reached the action is engaged. For example, if the count is 10, as soon as the signature is triggered 10 times the traffic would be blocked.

If the setting is "periodical", the FortiGate allows up to the value of the rate-count incidents where the signature is triggered during the rate-duration. For example, if the rate count is 100 and the duration is 60, the signature would need to be triggered 100 times in 60 seconds for the action to be engaged.

```
set rate-track <dest-ip | dhcp-client-mac | dns-domain | none | src-ip>
```

This setting allows the tracking of one of the protocol fields within the packet.

Geographic location filter

Place filters based on geographical location. Note that routes will not be installed if the resolved IPv6 address belongs to the country in the filter.

Any country entered for `geo-filter` will prevent all destination addresses that belong to that country from being installed into static routing table:

```
config webfilter {ips-urlfilter-setting | ips-urlfilter-setting6}
   edit <address>
      set geo-filter <country-name>
   next
end
```

Use the following diagnose command to list the IPv4 and/or IPv6 IP ranges of a specific country:

```
diagnose geoip {iprange6 | iprange} <country-name>
```

Enabling IPS packet logging

Packet logging saves the network packets containing the traffic matching an IPS signature to the attack log. The FortiGate unit will save the logged packets to wherever the logs are configured to be stored, whether memory, internal hard drive, a FortiAnalyzer unit, or the FortiGuard Analysis and Management Service.

You can enable packet logging in the filters. Use caution in enabling packet logging in a filter. Filters configured with few restrictions can contain thousands of signatures, potentially resulting in a flood of saved packets. This would take up a great deal of space, require time to sort through, and consume considerable system resources to process. Packet logging is designed as a focused diagnostic tool and is best used with a narrow scope.

Although logging to multiple FortiAnalyzer units is supported, packet logs are not sent to the secondary and tertiary FortiAnalyzer units. Only the primary unit receives packet logs.

To enable packet logging for a filter

1. Create a filter in an IPS sensor.
2. After creating the filter, right-click the filter, and select **Enable** in the **Packet Logging** column of the filter table.
3. Select the IPS sensor in the security policy that allows the network traffic the FortiGate unit will examine for the signature.

For information on viewing and saving logged packets, see Configuring packet logging options below.

IPS logging changes

IPS operations severely affected by disk logging are moved out of the quick scanning path, including logging, SNMP trap generation, quarantine, etc.

Scanning processes are dedicated to nothing but scanning, which results in more evenly distributed CPU usage. Slow (IPS) operations are taken care of in a dedicated process, which usually stays idle.

Setting `packet-log-history` to a value larger than `1` can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.

Other IPS examples

Configuring basic Intrusion Prevention

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable IPS on a FortiGate unit located in a satellite office. The satellite office contains only Windows clients.

Creating an IPS sensor

Most IPS settings are configured in an IPS sensor. IPS sensors are selected in firewall policies. This way, you can create multiple IPS sensors, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one IPS sensor.

To create an IPS sensor— GUI

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select the **Create New** icon in the top of the Edit IPS Sensor window.
3. In the **Name** field, enter `basic_ips`.
4. In the **Comments** field, enter `IPS for Windows clients`.
5. Select **OK**.

6. Select the **Create New** drop-down to add a new component to the sensor and for the **Sensor Type** choose **Filter** Based.
7. In the Filter Options choose the following:
   a. For **Severity**: select all of the options
   b. For **Target**: select **Client** only.
   c. For **OS**: select **Windows** only.
8. For the **Action** leave as the default.
9. Select **OK** to save the filter.
10. Select **OK** to save the IPS sensor.

To create an IPS sensor — CLI

```
config ips sensor
   edit basic_ips
      set comment "IPS for Windows clients"
         config entries
            edit 1
               set location client
               set os windows
            end
         end
      end
   end
```

Selecting the IPS sensor in a security policy

An IPS sensor directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an IPS sensor is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the IPS sensor in a security policy — GUI

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select a policy.
3. Select the **Edit** icon.
4. Enable the **IPS** option under **Security Profiles**.
5. Select the preferred IPS sensor from the dropdown menu.
6. Select **OK** to save the security policy.

To select the IPS sensor in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set ips-sensor basic_ips
   end
```

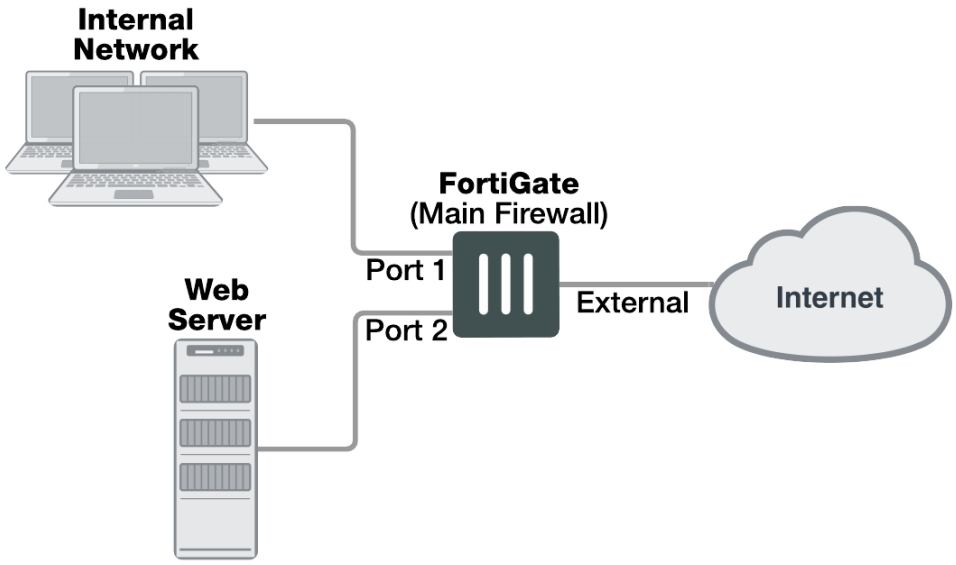
The IPS sensor in this example is `basic_ips`. All traffic handled by the security policy you modified will be scanned for attacks against Windows clients. A small office may have only one security policy configured. If you have multiple policies, consider enabling IPS scanning for all of them.

Using IPS to protect your web server

Many companies have web servers and they must be protected from attack. Since web servers must be accessible, protection is not as simple as blocking access. IPS is one tool your FortiGate unit has to allow you to protect your network.

In this example, we will configure IPS to protect a web server. As shown below, a FortiGate unit protects a web server and an internal network. The internal network will have its own policies and configuration but we will concentrate on the web server in this example.

A simple network configuration



The FortiGate unit is configured with:

- a virtual IP to give the web server a unique address accessible from the Internet.
- a security policy to allow access to the web server from the Internet using the virtual IP.

To protect the web server using intrusion prevention, you need to create an IPS sensor, populate it with filters, then enable IPS scanning in the security policy.

To create an IPS sensor

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select **Create New**.
3. Enter `web_server` as the name of the new IPS sensor.
4. Select **OK**.

The new IPS sensor is created but it has no filters, and therefore no signatures are included.

The web server operating system is Linux, so you need to create a filter for all Linux server signatures.

To create the Linux server filter

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select the `web_server` IPS sensor and select the **Edit** icon.

3. In the **Pattern Based Signatures and Filters** section, select **Create New**.
4. For **Sensor Type**, select **Filter Based.**
5. For Filter **Options**.
6. In the Filter Options choose the following:
   a. For **Severity**: select all of the options
   b. For **Target**: select **server** only.
   c. For **OS**: select **Linux** only.
7. Select **OK**.

The filter is saved and the IPS sensor page reappears. In the filter list, find the **Linux Server** filter and look at the value in the **Count** column. This shows how many signatures match the current filter settings. You can select the **View Rules** icon to see a listing of the included signatures.

To edit the security policy

1. Go to **Policy & Objects > IPv4 Policy** select security policy that allows access to the web server, and select the **Edit** icon.
2. Enable IPS option and choose the `web_server` IPS sensor from the list.
3. Select **OK**.

Since IPS is enabled and the `web_server` IPS sensor is specified in the security policy controlling the web server traffic, the IPS sensor examines the web server traffic for matches to the signatures it contains.

Create and test a packet logging IPS sensor

In this example, you create a new IPS sensor and include a filter that detects the EICAR test file and saves a packet log when it is found. This is an ideal first experience with packet logging because the EICAR test file can cause no harm, and it is freely available for testing purposes.

Create an IPS senor

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select **Create New**.
3. Name the new IPS sensor `EICAR_test`.
4. Select **OK**.

Create an entry

1. Select the **Create New**.
2. For **Sensor Type** choose **Specify Signatures**.
3. Rather than search through the signature list, use the name filter by selecting the search icon over the header of the **Signature** column.
4. Enter `EICAR` in the Search field.
5. Highlight the `Eicar.Virus.Test.File` signature by clicking on it.
6. Select **Block** as the **Action** for the `EICAR test` sensor in the **IPS Signatures** table.
7. Enable **Packet Logging.**
8. Select **OK** to save the IPS sensor.

Add the IPS sensor to the security policy allowing Internet access

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select the security policy that allows you to access the Internet.
3. Select the **Edit** icon.
4. Go to **Security Profiles** and enable **IPS** and choose `EICAR test` from the available IPS sensors..
5. Enable **Log Allowed Traffic** and select **All Sessions**.
6. Select **OK**.

With the IPS sensor configured and selected in the security policy, the FortiGate unit blocks any attempt to download the EICAR test file.

Test the IPS sensor

1. Using your web browser, go to http://www.eicar.org/anti_virus_test_file.htm.
2. Scroll to the bottom of the page and select **eicar.com** from the row labeled as using the standard HTTP protocol.
3. The browser attempts to download the requested file and,
   - If the file is successfully downloaded, the custom signature configuration failed at some point. Check the custom signature, the IPS sensor, and the firewall profile.
   - If the download is blocked with a high security alert message explaining that you're not permitted to download the file, the EICAR test file was blocked by the FortiGate unit antivirus scanner before the IPS sensor could examine it. Disable antivirus scanning and try to download the EICAR test file again.
   - If no file is downloaded and the browser eventually times out, the custom signature successfully detected the EICAR test file and blocked the download.

Viewing the packet log

1. Go to **Log & Report > Forward Traffic**.
2. Locate the log entry that recorded the blocking of the EICAR test file block. The Message field data will be `tools: EICAR.AV.Test.File.Download`.
3. Select the **View Packet Log** icon in the **Packet Log** column.
4. The packet log viewer is displayed.

Configuring a Fortinet Security Processing module

The Example Corporation has a web site that is the target of SYN floods. While they investigate the source of the attacks, it's very important that the web site remain accessible. To enhance the ability of the company's FortiGate-100D to deal with SYN floods, the administrator will install an ASM-CE4 Fortinet Security Processing module and have all external access to the web server come though it.

The security processing modules not only accelerate and offload network traffic from the FortiGate unit's processor, but they also accelerate and offload security and content scanning. The ability of the security module to accelerate IPS scanning and DoS protection greatly enhances the defense capabilities of the FortiGate-100D.

Assumptions

As shown in other examples and network diagrams throughout this document, the Example Corporation has a pair of FortiGate-100D units in an HA cluster. To simplify this example, the cluster is replaced with a single

FortiGate-100D.

An ASM-CE4 is installed in the FortiGate-100D.

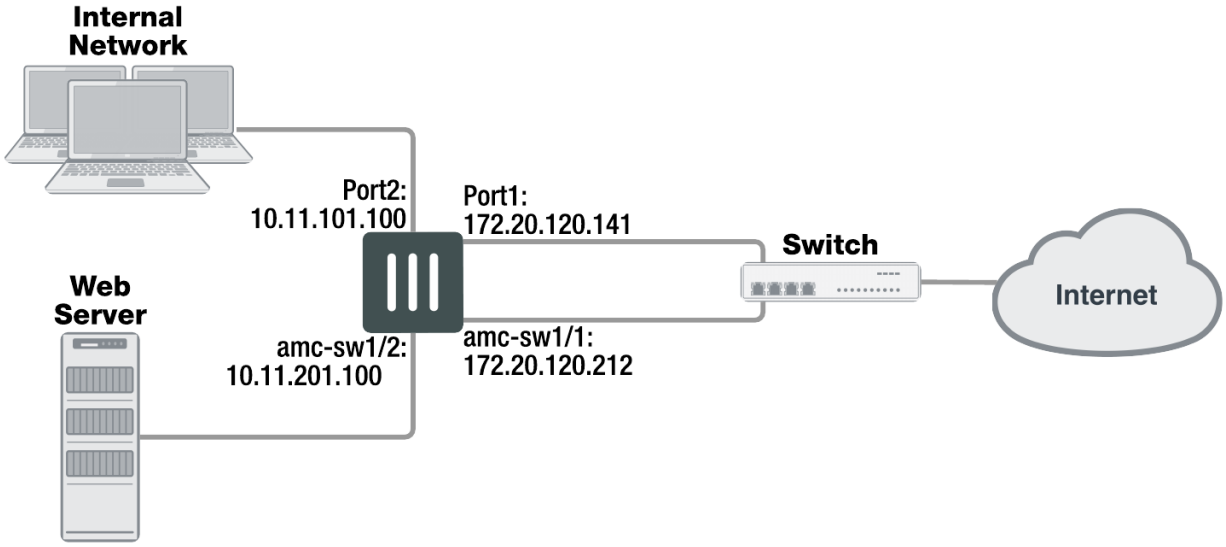
The network is configured as shown below.

Network configuration

The Example Corporation network needs minimal changes to incorporate the ASM-CE4. Interface amc-sw1/1 of the ASM-CE4 is connected to the Internet and interface amc-sw1/1 is connected to the web server.

Since the main office network is connected to port2 and the Internet is connected to port1, a switch is installed to allow both port1 and amc-sw1/1 to be connected to the Internet.

The FortiGate-100D network configuration



The switch used to connect port1 and amc-sw1/1 to the Internet must be able to handle any SYN flood, all of the legitimate traffic to the web site, and all of the traffic to and from the Example Corporation internal network. If the switch can not handle the bandwidth, or if the connection to the service provider can not provide the required bandwidth, traffic will be lost.

Security module configuration

The Fortinet security modules come configured to give equal priority to content inspection and firewall processing. The Example Corporation is using a ASM-CE4 module to defend its web server against SYN flood attacks so firewall processing is a secondary consideration.

Use these CLI commands to configure the security module in ASM slot 1 to devote more resources to content processing, including DoS and IPS, than to firewall processing.

```
config system amc-slot
   edit sw1
      set optimization-mode fw-ips
      set ips-weight balanced
      set ips-p2p disable
      set ips-fail-open enable
      set fp-disable none
      set ipsec-inb-optimization enable
```

```
        set syn-proxy-client-timer 3
        set syn-proxy-server-timer 3
    end
```

These settings do not disable firewall processing. Rather, when the security module nears its processing capacity, it will chose to service content inspection over firewall processing.

Anti-spam filter

This section describes how to configure FortiGate email filtering for IMAP, POP3, and SMTP email. Email filtering includes both spam filtering and filtering for any words or files you want to disallow in email messages. If your FortiGate unit supports SSL content scanning and inspection, you can also configure spam filtering for IMAPS, POP3S, and SMTPS email traffic.

The Anti-Spam security profile is only available when operating the FortiGate in proxy-based inspection.

The following topics are included in this section:

Anti-spam concepts

You can configure the FortiGate unit to manage unsolicited commercial email by detecting and identifying spam messages from known or suspected spam servers.

The FortiGuard Anti-Spam service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools, to detect and block a wide range of spam messages. Using FortiGuard Anti-Spam profile settings, you can opt to filter with IP address checking, URL checking, email checksum checking, detection of phishing URLs in email, and spam submission. Updates to the IP reputation and spam signature databases are provided continuously via the global FortiGuard Distribution Network.

At the FortiGuard Anti-Spam service page on the FortiGuard Labs website, you can find out whether an IP address is blacklisted in the FortiGuard Anti-Spam IP reputation database, or whether a URL or email address is in the signature database.

Anti-spam techniques

The FortiGate unit has a number of techniques available to help detect spam. Some use the FortiGuard Anti-Spam service and require a subscription. The remainder use your DNS servers or use lists that you must maintain.

Black white list

These are the types of black white lists available. They include:

- **IP/Netmask**
  The FortiGate unit compares the IP address of the client delivering the email to the addresses in the IP address

black / white list specified in the email filter profile. If a match is found, the FortiGate unit will take the action configured for the matching black / white list entry against all delivered email.
The default setting of the `smtp-spamhdrip` CLI command is `disable`. If enabled, the FortiGate unit will check all the IP addresses in the header of SMTP email against the specified IP address black / white list.

- **Email Wildcard**
  The FortiGate unit compares the sender email address, as shown in the message header and envelope MAIL FROM, to the pattern in the patterned field. The wildcard symbol is used in the place of characters in the address that may vary from the pattern. If a match is found, the FortiGate unit will take the action configured for the matching black / white list entry.
- **Email Regular Expression**
  The FortiGate unit compares the sender email address, as shown in the message envelope MAIL FROM, to the pattern in the patterned field. The regular expression that can be used is much more sophisticated than a simple wildcard variable. If a match is found, the FortiGate unit will take the action configured for the matching black/white list entry.

Pattern

The pattern field is for entering the identifying information that will enable the filter to correctly identify the email messages.

- If the type is IP/Netmask the filter will be an IP address with a subnet mask.
- If the type is Email Wildcard the filter will be an email address with a wildcard symbol in place of the variable characters. For example *.example.com or fred@*.com.
- If the type is Email Regular Expression, regular expression can be used to create a more granular filter for email addresses. For example, ^[_a-z0-9-]+(\.[_a-z0-9-]+)*@(example|xmple|examp).(com|org|net) could be used filter based on a number of combinations of email domain names.

Action

- **Tag**
  If this is the selected action, the email will be allowed through but it will be tagged with an indicator that clearly marks the email as spam.
- **Pass**
  If this is the selected action, the email will be allowed to go through to its destination on the assumption that the message is not spam.
- **Discard**
  If this is the selected action, the email will be dropped at the before reaching its destination.

Status

Indicates whether this particular list is enabled or disabled.

Banned word check

When you enable banned word checking, your FortiGate unit will examine the email message for words appearing in the banned word list specified in the Anti-Spam profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the Anti-Spam profile, your FortiGate unit will treat the message as spam.

When determining the banned word score total for an email message, each banned word score is added once no matter how many times the word appears in the message. Use the command `config spamfilter bword` to

add an email banned word list. Use the command `config spamfilter profile` to add a banned word list to an Anti-Spam profile.

How content is evaluated

Every time the banned word filter detects a pattern in an email message, it adds the pattern score to the sum of scores for the message. You set this score when you create a new pattern to block content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the total score equals or exceeds the threshold, the email message is considered as spam and treated according to the spam action configured in the email filter profile. The score for each pattern is counted only once, even if that pattern appears many times in the email message. The default score for banned word patterns is 10 and the default threshold is 10. This means that by default, an email message is blocked by a single match.

A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.

For example, the FortiGate unit scans an email message that contains only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the email message.”

Banned word pat-tern	Pattern type	Assigned score	Score added to the sum for the entire page	Comment
word	Wildcard	20	20	The pattern appears twice but multiple occurrences are only counted once.
word phrase	Wildcard	20	0	Although each word in the phrase appears in the message, the words do not appear together as they do in the pattern. There are no matches.
word*phrase	Wildcard	20	20	The wildcard represents any number of any character. A match occurs as long as “word” appears before “phrase” regardless of what is in between them.
mail*age	Wildcard	20	20	Since the wildcard character can represent any characters, this pattern is a match because “email message” appears in the message.

In this example, the message is treated as spam if the banned word threshold is set to 60 or less.

Adding words to a banned word list

When you enter a word, set the `Pattern-type` to wildcards or regular expressions.

Wildcard uses an asterisk (“*”) to match any number of any character. For example, re* will match all words starting with “re”.

Regular expression uses Perl regular expression syntax. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.

DNS-based Blackhole List (DNSBL)

A DNSBL is a list of IP addresses, usually maintained by a third party, which are identified as being associated with spamming.

FortiGuard Anti-spam Service.

FortiGuard IP address check

The FortiGate unit queries the FortiGuard Anti-Spam Service to determine if the IP address of the client delivering the email is blacklisted. A match will cause the FortiGate unit to treat delivered messages as spam.

The default setting of the `smtp-spamhdrip` CLI command is `disable`. When you enable FortiGuard IP address checking, your FortiGate unit will submit the IP address of the client to the FortiGuard service for checking. If the IP address exists in the FortiGuard IP address black list, your FortiGate unit will treat the message as spam.

FortiGuard URL check

When you enable FortiGuard URL checking, your FortiGate unit will submit all URLs appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL black list, your FortiGate unit will treat the message as spam.

FortiGuard email checksum check

When you enable FortiGuard email checksum checking, your FortiGate unit will submit a checksum of each email message to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum black list, your FortiGate unit will treat the message as spam.

Detect phishing URLs in email

When you enable FortiGuard phishing URL detection, your FortiGate unit will submit all URL hyperlinks appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL phishing list, your FortiGate unit will remove the hyperlink from the message. The URL will remain in place, but it will no longer be a selectable hyperlink.

FortiGuard spam submission

Spam submission is a way you can inform the FortiGuard Anti-Spam service of non-spam messages incorrectly marked as spam. When you enable this setting, the FortiGate unit adds a link to the end of every message marked as spam. You then select this link to inform the FortiGuard Anti-Spam service when a message is incorrectly marked.

Trusted IP addresses

A list of IP addresses that are trusted by the FortiGate is created. Any email traffic coming in from these IP address will be exempted to perform IP based check, such as DNSBL/RBL, FortiShield SPAM IP or locally defined IP black list check.

If the FortiGate unit sits behind a company's Mail Transfer Units, it may be unnecessary to check email IP addresses because they are internal and trusted. The only IP addresses that need to be checked are those from

outside of the company. In some cases, external IP addresses may be added to the list if it is known that they are not sources of spam.

MIME header

This feature filters by the MIME header. MIME header settings are configured in a separate part of the command tree but MIME header filtering is enabled within each profile.

HELO DNS lookup

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. The FortiGate unit takes the domain name specified by the client in the HELO and does a DNS lookup to determine if the domain exists. If the lookup fails, the FortiGate unit determines that any messages delivered during the SMTP session are spam.

The HELO DNS lookup is available only for SMTP traffic.

Return email DNS check

The FortiGate unit performs a DNS lookup on the If no such record exists, the message is treated as spam.

When you enable return email DNS checking, your FortiGate unit will take the domain in the reply-to email address and reply-to domain and check the DNS servers to see if there is an A or MX record for the domain. If the domain does not exist, your FortiGate unit will treat the message as spam.

Configuring Anti-spam

FortiGuard email filtering techniques us FortiGuard services to detect the presence of spam among your email. A FortiGuard subscription is required to use the FortiGuard email filters. To enable email filtering an email filter needs to be created and then the filter needs to be associated with a security policy.

The Anti-Spam security profile is only available when operating the FortiGate in proxy-based inspection.

The filter can be created as follows:

- Go to **Security Profiles > Anti-Spam**.
  - Select the **Create New** icon (a plus symbol in a circle in the upper right hand corner).
  - Select the **List** icon (a page symbol in the upper right hand corner) and in the new window select **Create New**.

An existing filter can be edited as follows:

- Go to **Security Profiles > Anti-Spam**.
  - Select the filter that you wish to edit from the dropdown menu in the upper right corner.
  - Select the List icon (a page symbol in the upper right hand corner) and select the filter that you wish to edit from the list.

Once you are in the proper **Edit Anti-Spam Profile** window, you can enter a name in the Name field if it's a new filter.

The Comments field is for a description or other information that will assist in understanding the function or purpose of the this particular filter.

Before any of the other features or options of the filter appear the checkbox next to Enable Spam Detection and Filtering must be checked.

Spam detection by protocol

This matrix includes three rows that represent the email protocols IMAP, POP3 and SMTP.

There are also columns for:

Spam Action

For the client protocols, IMAP and POP3 the options are:

- **Tag** - This action will insert a tag into the email somewhere so that when the recipients view the email they will be warned that it is likely a spam.
- **Pass** - This action will allow any emails marked as spam to pass through without change. If this option is chosen, the Tag comments will be greyed out.

For the transfer protocol, SMTP, the options are:

- **Tag** - This action will insert a tag into the email somewhere so that when the recipients view the email they will be warned that it is likely a spam.
- **Discard** - The action will drop the email before it reaches its destination.
- **Pass** - This action will allow any emails marked as spam to pass through without change. If this option is chosen, the Tag comments will be greyed out.

Tag Location

- **Subject** - The contents of the Tag Format will be inserted into the subject line. The subject line is the most commonly used.
- **MIME** - The contents of the Tag Format will be inserted in with the MIME header header.

Tag Format

The contents of this field will be entered into the tag location specified. The most common tag is something along the lines of [Spam] or **SPAM**

FortiGuard spam filtering

The options in the section are ones that require a FortiGuard subscription.

The options available in this section, to be selected by checkbox are:

- IP Address Check
- URL Check
- Detect Phishing URLs in Email
- Email Checksum Check
- Spam Submission

Local spam filtering

The options in the section are ones can be managed on the local device without the need for a FortiGuard subscription.

The options available in this section, to be selected by checkbox are:

- HELO DNS Lookup
- Return Email DNS Check
- Black White List - checking this option will produce a table that can be edited to create a number of black / white lists that can be separately configured and enabled.

Another local spam filter profile option that can only be configured in the CLI is the `bannedword`.check. To configure this, enter the following commands in the CLI:

```
config spamfilter profile
   edit <filter_name>
      set options bannedword
      set spam-bword-table 1
   next
end
```

See the section on banned word checking for more information on how content is evaluated.

Order of spam filtering

The FortiGate unit checks for spam using various filtering techniques. The order in which the FortiGate unit uses these filters depends on the mail protocol used.

Filters requiring a query to a server and a reply (FortiGuard Anti-Spam service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each spam filter passes the email to the next if no matches or problems are found. If the action in the filter is **Mark as Spam**, the FortiGate unit tags the email as spam according to the settings in the email filter profile.

For SMTP and SMTPS, if the action is **Discard**, the email message is discarded or dropped.

If the action in the filter is **Mark as Clear**, the email is exempt from any remaining filters. If the action in the filter is **Mark as Reject**, the email session is dropped.

Order of SMTP and SMTPS spam filtering

The FortiGate unit scans SMTP and SMTPS email for spam in a specific order, depending on whether or not the local override feature has been enabled. By default, local override is disabled on the FortiGate. Enabling local override will give priority to local spam filters.

You can enable local override with the CLI command `set local-override {enable | disable}` when configuring a spamfilter profile. Enable this command to override SMTP or SMTPS remote check, which includes IP RBL check, IP FortiGuard AntiSpam check and HELO DNS check, with the locally defined black/white antispam list.

SMTPS spam filtering is available on FortiGate units that support SSL content scanning and inspection.

Enabling local override of Anti-Spam filter

CLI Syntax

```
config spamfilter profile
   edit <filter_name>
      set spam-filtering enable
      set options spambwl spamfsip spamfsurl spamhelodns spamfsphish
      config smtp
         set local-override enable
      end
      set spam-bwl-table 1
   next
end
```

Order of SMTP and SMTPS spam filtering with local-override disabled

1. HELO DNS Lookup, Last Hop IP check against ORDBL
2. Return email DNS check, FortiGuard email checksum check, FortiGuard URL check, FortiGuard IP address check, Phishing URLs detection
3. Last Hop IP check local black/white list (BWL)
4. Envelope Address check local BWL
5. Headers IPs local BWL
6. Headers email address local BWL, MIME header checks based on local list of patterns (mheader)
7. Banned words (subject first, then body) based on local BWL (bword)

Order of SMTP and SMTPS spam filtering with local-override enabled

1. Last Hop IP check local black/while list (BWL)
2. Envelope Address check local BWL
3. Headers IPs local BWL, MIME header checks based on local list of patterns (mheader)
4. Headers email address local BWL
5. Banned words (subject first, then body) based on local list of patterns (bword)
6. HELO DNS Lookup, Last Hop IP check against ORDBL
7. Return email DNS check, FortiGuard email checksum check, FortiGuard URL check, FortiGuard IP address checks, Phishing URLs detection

Order of IMAP, POP3, IMAPS and POP3S spam filtering

The FortiGate unit scans IMAP, POP3, IMAPS and POP3S email for spam in the order given below. IMAPS and POP3S spam filtering is available on FortiGate units that support SSL content scanning and inspection.

1. MIME headers check, E-mail address BWL check
2. Banned word check on email subject
3. IP BWL check
4. Banned word check on email body
5. Return email DNS check, FortiGuard Antispam email checksum check, FortiGuard Antispam URL check, DNSBL & ORDBL check.

Spam actions

When spam is detected, the FortiGate unit will deal with it according to the **Spam Action** setting in the anti-spam profile. Note that POP3S, IMAPS and SMTPS spam filtering is available only on FortiGate units that support SSL content scanning and inspection. POP3, IMAP, POP3S and IMAPS mail can only be tagged. SMTP and SMTPS mail can be set to **Discard** or **Tagged**:

Discard

When the spam action is set to **Discard**, messages detected as spam are deleted. No notification is sent to the sender or recipient.

Pass

When the spam action is set to **Pass**, the spam filter is disabled for the related protocol.

Tag

When the spam action is set to **Tag**, messages detected as spam are labeled and delivered normally. The text used for the label is set in the **Tag Format** field and the label is placed in the subject or the message header, as set with the **Tag Location** option.

Anti-spam examples

Configuring simple Anti-spam protection

Small offices, whether they are small companies, home offices, or satellite offices, often have very simple needs. This example details how to enable Anti-Spam protection on a FortiGate unit located in a satellite office.

Creating an email filter profile

Most Anti-Spam settings are configured in an Anti-Spam profile. Anti-Spam profiles are selected in firewall policies. This way, you can create multiple Anti-Spam profiles, and tailor them to the traffic controlled by the security policy in which they are selected. In this example, you will create one Anti-Spam profile.

To create an Anti-Spam profile — web-based manager

1. Go to **Security Profiles > Anti-Spam**.
2. Select the **Create New** icon in the Edit Anti-Spam Profile window title.
3. In the **Name** field, enter `basic_anti-spam`
4. Select **Enable Spam Detection and Filtering**.
5. Ensure that **IMAP**, **POP3**, and **SMTP** are selected in the header row.

   These header row selections enable or disable examination of each Anti-Spam type. When disabled, the email traffic of that type is ignored by the FortiGate unit and no Anti-Spam options are available.

6. Under **FortiGuard Spam Filtering**, enable **IP Address Check**.
7. Under **FortiGuard Spam Filtering**, enable **URL Check**.
8. Under **FortiGuard Spam Filtering**, enable **E-mail Checksum Check**.
9. Select **OK** to save the email filter profile.

To create an Anti-spam profile — CLI

```
config spamfilter profile
   edit basic_anti-spam
      set options spamfsip spamfsurl spamfschksum
   end
```

Selecting the Anti-spam profile in a security policy

An Anti-Spam profile directs the FortiGate unit to scan network traffic only when it is selected in a security policy. When an Anti-Spam profile is selected in a security policy, its settings are applied to all the traffic the security policy handles.

To select the Anti-Spam profile in a security policy — web-based manager

1. Go to **Policy & Objects > IPv4 Policy**.
2. Create a new or edit a policy.
3. Turn on Anti-Spam.
4. Select the `basic_anti-spam` profile from the list.
5. Select **OK** to save the security policy.

To select the Anti-spam profile in a security policy — CLI

```
config firewall policy
   edit 1
      set utm-status enable
      set profile-protocol-options default
      set spamfilter-profile basic_anti-spam
   end
```

IMAP, POP3, and SMTP email traffic handled by the security policy you modified will be scanned for spam. Spam messages have the text “Spam” added to their subject lines. A small office may have only one security policy configured. If you have multiple policies, consider enabling spam scanning for all of them.

Blocking email from a user

Employees of the Example.com corporation have been receiving unwanted email messages from a former client at a company called example.net. The client’s email address is client@example.net. All ties between the company and the client have been severed, but the messages continue. The FortiGate unit can be configured to prevent these messages from being delivered.

To enable Anti-Spam

1. Go to **Security Profiles > Anti-Spam**.
2. Select the Anti-Spam profile that is used by the firewall policies handling email traffic from the Anti-Spam profile drop down list.
3. In the row **Tag Location**, select **Subject** for all three mail protocols.

4. In the row **Tag Format**, enter `SPAM:` in all three fields.
   This means that normal spam will be tagged in the subject line.
5. Select **Enable Spam Detection and Filtering**.
6. Under **Local Spam Filtering**, enable **Black White List** and select **Create New**.
7. In the Black White List widget, select **Create New**.
8. Select **Email Address Wildcard**.
9. Enter `client@example.net` in the **Pattern** field.
   - If you wanted to prevent everyone's email from the client's company from getting through you could have used *@example.net instead.
10. Set the **Action** as **Mark as Spam**.
11. Set the **Status** to **Enable**.
12. Confirm that the SMTP protocol action is set to **Discard**.
13. Select **OK**.

Now that the email address list is created, you must enable the email filter in the Anti-Spam profile.

When this Anti-Spam profile is selected in a security policy, the FortiGate unit will reject any email message from an address ending with @example.net for all email traffic handled by the security policy.

Data leak prevention

The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through the FortiGate unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the FortiGate unit.

This section describes how to configure the DLP settings. DLP can only be configured for FortiGate units in proxy-based inspection.

The following topics are included:

Data leak prevention concepts

Data leak prevention examines network traffic for data patterns you define through the use of the GUI and CLI commands. The DLP feature is broken down into a number of parts. Note, DLP is not available in flow-based inspection.

DLP sensor

A DLP sensor is a package of filters. To use DLP, you must enable it in a security policy and select the DLP sensor to use. The traffic controlled by the security policy will be searched for the patterns defined in the filters contained in the DLP sensor. Matching traffic will be passed or blocked according to how you configured the filters.

DLP filter

Each DLP sensor has one or more filters configured within it. Filters can examine traffic for known files using DLP fingerprints, for files of a particular type or name, for files larger than a specified size, for data matching a specified regular expression, or for traffic matching an advanced rule or compound rule.

DLP filter actions

You can configure the action taken when a match is detected. The actions include:

- Allow
- Log Only
- Block
- Quarantine IP address

Log Only is enabled by default.

Allow

No action is taken even if the patterns specified in the filter are matched.

Log Only

The FortiGate unit will take no action on network traffic matching a rule with this action. The filter match is logged, however. Other matching filters in the same sensor may still operate on matching traffic.

Block

Traffic matching a filter with the block action will not be delivered. The matching message or download is replaced with the data leak prevention replacement message.

Quarantine IP Address/ Source IP ban

Starting in FortiOS 5.2, the quarantine, as a place where traffic content was held in storage so it couldn't interact with the network or system, was removed. The term quarantine was kept to describe preventing selected source IPs from interacting with the network and protected systems. This source IP ban is kept in the kernel rather than in any specific application engine and can be queried by APIs. The features that can use the APIs to access and use the banned source IP addresses are antivirus, DLP, DoS and IPS. Both IPv4 and IPv6 version are included in this feature.

If the **quarantine-ip** action is used, the additional variable of expiry time will become available. This variable determines for how long the source IP address will be blocked. In the GUI it is shown as a field before minutes. In the CLI the option is called `expiry` and the duration is in the format `<###d##h##m>`. The maximum days value is 364. The maximum hour value is 23 and the maximum minute value is 59. The default is 5 minutes.

If a DLP sensor has contains a DLP filter with action set to **Allow** certain files and another DLP filter with action set to **Block** those same files, then the order of the filters within that sensor will determine which action is taken first.

Configuring using the CLI

To configure the DLP sensor to add the source IP address of the sender of a protected file to the quarantine or list of banned source IP addresses edit the DLP Filter, use these CLI commands:

```
config dlp sensor
   edit <sensor name>
      config filter
         edit <id number of filter>
            set action quarantine-ip
            set expiry 5m
            end
         end
```

Preconfigured sensors

A number of preconfigured sensors are provided with your FortiGate unit. These can be edited to more closely match your needs.

Two of the preconfigured sensors with filters ready for you to enable are:

- Credit-Card - This sensor logs the traffic, both files and messages, that contain credit card numbers in the formats used by American Express, MasterCard and Visa.
- SSN-Sensor - This sensor logs the traffic, both files and messages, that contain Social Security Numbers with the exception of those that are WebEx invitation emails.

These rules affect only unencrypted traffic types. If you are using a FortiGate unit that can decrypt and examine encrypted traffic, you can enable those traffic types in these rules to extend their functionality if required.

Before using the rules, examine them closely to ensure you understand how they will affect the traffic on your network.

DLP document fingerprinting

One of the DLP techniques to detect sensitive data is fingerprinting (also called document fingerprinting). Most DLP techniques rely on you providing a characteristic of the file you want to detect, whether it's the file type, the file name, or part of the file contents. Fingerprinting is different in that you provide the file itself. The FortiGate unit then generates a checksum fingerprint and stores it. The FortiGate unit generates a fingerprint for all files detected in network traffic, and it is compared to all of the fingerprints stored in its fingerprint database. If a match is found, the configured action is taken.

The document fingerprint feature requires a FortiGate unit with internal storage.

Any type of file can be detected by DLP fingerprinting and fingerprints can be saved for each revision of your files as they are updated.

To use fingerprinting you:

- select the documents to be fingerprinted
- add fingerprinting filters to DLP sensors
- add the sensors to firewall policies that accept the traffic to which to apply fingerprinting.

Fingerprinting

Fingerprint scanning allows you to create a library of files for the FortiGate unit to examine. It will create checksum fingerprints so each file can be easily identified. Then, when files appear in network traffic, the FortiGate will generate a checksum fingerprint and compare it to those in the fingerprint database. A match triggers the configured action.

You must configure a document source or uploaded documents to the FortiGate unit for fingerprint scanning to work.

Fingerprinted documents

The FortiGate unit must have access to the documents for which it generates fingerprints.

Configuring the document source

To configure a DLP fingerprint document source in FortiOS 5.6.0, you must use CLI commands.

```
config dlp fp-doc-source
   edit <name_str>
      set name <string>
      set server-type {smb}
      set server <string>
      set period {none | daily | weekly | monthly}
      set vdom {mgmt | current}
      set scan-subdirectories {enable | disable}
      set remove-deleted {enable | disable}
      set keep-modified {enable | disable}
      set username <string>
      set password <password>
      set file-path <string>
      set file-pattern <string>
      set sensitivity <string>
      set tod-hour <integer>
      set tod-min <integer>
      set weekday {sunday | monday | tuesday | wednesday | thursday | friday | saturday}
      set date <integer>
   end
```

Configuring a DLP fingerprint sensor

To configure a DLP fingerprint sensor in FortiOS 5.6.0, you must use CLI commands.

```
config dlp sensor
   edit <sensor name>
      config filter
         edit <id number of filter>
            set proto {smtp | pop3 | imap http-get | http-post | ftp | nntp | mapi}
            set filter-by fingerprint
            set fp-sensitivity { critical | private | warning}
            set action {allow | log-only | block | ban | quarantine-ip | quarantine-
                port}
         next
      end
   next
```

Once you have set the document source and configured the DLP sensor for fingerprinting, add the DLP sensor to the applicable firewall policy. This can be done through the GUI.

File size

This filter-type checks for files exceeding a configured size. All files larger than the specified size are subject to the configured action. The value of the field is measured in kilobytes (KB).

DLP filtering by specific file types

File filters use file filter lists to examine network traffic for files that match either file names or file types. For example, you can create a file filter list that will find files called secret.* and also all JPEG graphic files. You can create multiple file filter lists and use them in filters in multiple DLP sensors as required.

Specify File Types is a DLP option that allows you to block files based on their file name or their type.

- **File types** are a means of filtering based on examination of the file contents, regardless of the file name. If you block the file type **Archive (zip)**, all zip archives are blocked even if they are renamed with a different file extension. The FortiGate examines the file contents to determine what type of file it is and then acts accordingly.
- **File Name patterns** are a means of filtering based purely on the names of files. They may include wildcards (*). For example, blocking `*.scr` will stop all files with an `.scr` file extension, which is commonly used for Windows screen saver files. Files trying to pass themselves off as Windows screen saver files by adopting the file-naming convention will also be stopped.
  - Files can specify the full or partial file name, the full or partial file extension, or any combination. File pattern entries are not case sensitive. For example, adding `*.exe` to the file pattern list also blocks any files ending with `.exe`.
  - Files are compared to the enabled file patterns from top to bottom, in list order.

If DLP detects a file inside an archive that should be blocked, the entire archive will be blocked.

Watermarking

Watermarking is essentially marking files with a digital pattern to mark the file as being proprietary to a specific company. Fortinet provides a Linux-based utility that applies a digital watermark to files. The utility adds a small (approx. 100 byte) pattern to the file that is recognized by the DLP watermark filter. The pattern is invisible to the end user.

When watermarking a file it should be verified that the pattern matches up to a category found on the FortiGate firewall. For example, if you are going to watermark a file with the sensitivity level of “Secret” you should verify that “Secret” is a sensitivity level that has been assigned in the FortiGate unit.

Watermark Sensitivity

If you are using watermarking on your files you can use this filter to check for watermarks that correspond to sensitivity categories that you have set up.

The Corporate Identifier is to make sure that you are only blocking watermarks that your company has place on the files, not watermarks with the same name by other companies.

Software Versions

Before planning on using watermarking software it is always best to verify that the software will work with your OS. Currently, the only utility available to watermark files is a Linux-based command line tool. It is available for download from the Fortinet Customer Service & Support website, with a valid support contract and access to the site. To access the file:

1. Sign into the Fortinet Customer Service & Support website.
2. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
3. Navigate to the image file path for /FortiGate / v5.00 / 5.0 / WATERMARK
4. Download the file **fortinet-watermark-linux.out**.

File types

The watermark utility does not work with every file type. The following file types are supported by the watermark tool: .txt; .pdf; .doc; .xls; .ppt; .docx; pptx; and, .xlsx.

Syntax of the watermark utility

The tool is executed in a Linux environment by passing in files or directories of files to insert a watermark.

USAGE:

```
watermark_linux_amd64 <options> -f <file name> -i <identifier> -l <sensitivity level>
watermark_linux_amd64 <options> -d <directory> -i <identifier> -l <sensitivity level>
```

Options:

```
-h print help
-I inplace watermarking (don't copy file)
-o output file (or directory in directory mode)
-e encode <to non-readable>
-i add watermark identifier
-l add watermark sensitivity level
-D delete watermark identifier
-L delete watermark sensitivity level
```

Regular expression

The FortiGate unit checks network traffic for the regular expression specified in a regular expression filter. The regular expression library used by Fortinet is a variation of a library called PCRE (Perl Compatible Regular Expressions). A number of these filters can be added to a sensor making a sort of ‘dictionary’ subset within the sensor.

Some other, more limited DLP implementations, use a list of words in a text file to define what words are searched for. While the format used here is slightly different than what some people are used to, the resulting effect is similar. Each regular expression filter can be thought of as a more versatile word to be searched against. In this dictionary (or sensor), the list of words is not limited to just predefined words. It can include expressions that accommodate complex variations on those words and even target phrases. Another advantage of the individual filter model of this dictionary over the list is that each word can be assigned its own action, making this implementation much more granular.

Encrypted

This filter is a binary one. If the file going through the policy is encrypted the action is triggered.

Examining specific services

To assist in optimizing the performance of the firewall, the option exists to select which services or protocol traffic will be checked for the targeted content. This setting gives you a tool to save the resources of the FortiGate unit

by only using processing cycles on the relevant traffic. Just check the boxes associated with the service / protocol that you want to have checked for filter triggers.

Enable data leak prevention

DLP examines your network traffic for data patterns you specify. The FortiGate unit then performs an action based on the which pattern is found and a configuration set for each filter trigger.

DLP is not available in flow-based inspection.

General configuration steps

Follow the configuration procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create a DLP sensor.
   New DLP sensors are empty. You must create one or more filters in a sensor before it can examine network traffic.
2. Add one or more filters to the DLP sensor.
   Each filter searches for a specific data pattern. When a pattern in the active DLP sensor appears in the traffic, the FortiGate unit takes the action configured in the matching filter. Because the order of filters within a sensor cannot be changed, you must configure DLP in sequence.
3. Add the DLP sensor to one or more firewall policies that control the traffic to be examined.

Creating/editing a DLP sensor

DLP sensors are collections of filters. You must also specify an action for the filter when you create it in a sensor. Once a DLP sensor is configured, you add it to a security policy profile. Any traffic handled by that security policy will be examined according to the DLP sensor configuration.

DLP is not available in flow-based inspection.

To create/edit a DLP sensor in the GUI

1. Go to **Security Profiles > Data Leak Prevention**.
2. Choose whether you want to edit an existing sensor or create a new one.
   - The default sensor is the one displayed by default.
   - To edit an existing sensor, select it by either using the drop down menu in the upper right hand corner of the window or by selecting the **List** icon (the furthest right of the 3 icons in the upper right of the window, resembling a page with some lines on it), and then selecting the profile you want to edit from the list.
   - To create a new sensor, select the **Create New** icon (a plus sign within a circle) or the List icon and then select the Create New link in the upper left corner of the window that appears.
3. Enter a name in the **Name** field for any new DLP sensors.
4. Optionally, you may also enter a comment. The comment appears in the DLP sensor list and can remind you of the details of the sensor.
5. At this point you can add filters to the sensor (see adding filters to a DLP sensor) or select **OK** to save the sensor.

Without filters, the DLP sensor will do nothing.

Adding filters to a DLP sensor

Once you have created a DLP sensor, you need to add filters.

1. To add filters to a DLP sensor
2. Go to **Security Profiles > Data Leak Prevention**.
3. Select the sensor you wish to edit using the drop-down menu or the sensor list window.
4. Within the Edit DLP Sensor window select **Create New**. A New Filter window should pop up.
5. Select the type of filter. You can choose either **Messages** or **Files**, depending on which of these two are chosen different options will be available.

   Message filter will have these configuration options:
   - [radio button] Containing: [drop-down menu including: Credit Card # or SSN]
   - [radio button] Regular Expression [input field]

   Examine the following services:

   Web Access
   - HTTP-POST

   Email
   - [check box] SMTP
   - [check box] POP3
   - [check box] IMAP
   - [check box] MAPI

   Others
   - [check box] NNTP

   Action [from drop-down menu]
   - Allow
   - Log Only (default)
   - Block
   - Quarantine IP address

   Files filter will allow you to choose one of these options:
   - **Containing**: drop-down menu including: Credit Card # or SSN
   - **File Size** > [ ]KB files greater than the number of KB entered
   - Specify File Types
     File Types: [“Click to add…”drop-down menu of File extensions]
     File Name Patterns:[“Click to add…”drop-down menu]
   - [radio button] Regular Expression [input field]
   - [radio button] Encrypted

   Examine the following Services:

   Web Access

- [check box] HTTP-POST
- [check box] HTTP-GET

Email

- [check box] SMTP
- [check box] POP3
- [check box] IMAP
- [check box] MAPI

Others

- [check box] FTP
- [check box] NNTP

Action [from drop-down menu]

- Allow
- Log Only (default)
- Block
- Quarantine IP address

6. Select **OK**.
7. Repeat Steps 6 and 7 for each filter.
8. Select **Apply** to confirm the settings of the sensor.

If you have configured DLP to block IP addresses and if the FortiGate unit receives sessions that have passed through a NAT device, all traffic from that NAT device — not just traffic from individual users — could be blocked. You can avoid this problem by implementing authentication.

To view or modify the replacement message text, go to **System > Replacement Messages**.

DLP archiving

DLP is typically used to prevent sensitive information from getting out of your company network, but it can also be used to record network use. This is called DLP archiving. The DLP engine examines email, FTP, NNTP, and web traffic. Enabling archiving for rules when you add them to sensors directs the FortiGate unit to record all occurrences of these traffic types when they are detected by the sensor.

Since the archive setting is configured for each rule in a sensor, you can have a single sensor that archives only the things you want.

You can archive Email, FTP, HTTP, and session control content:

- Email content includes IMAP, POP3, and SMTP sessions. Email content can also include email messages tagged as spam by Email filtering. If your unit supports SSL content scanning and inspection, email content can also

include IMAPS, POP3S, and SMTPS sessions.

- HTTP content includes HTTP sessions. If your unit supports SSL content scanning and inspection HTTP content can also include HTTPS sessions.

DLP archiving comes in two forms: **Summary** and **Full**.

Summary archiving records information about the supported traffic types. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses the Web, every URL the user visits recorded. The result is a summary of all activity the sensor detected.

For more detailed records, use full archiving . When an email message is detected, the message itself, including any attachments, is archived. When a user accesses the Web, every page the user visits is archived. Far more detailed than a summary, full DLP archives require more storage space and processing.

Because both types of DLP archiving require additional resources, DLP archives are saved to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service (subscription required).

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the Fortinet configuration. The FortiGuard Analysis server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

Two sample DLP sensors are provided with DLP archiving capabilities enabled. If you select the `Content_Summary` sensor in a security policy, it will save a summary DLP archive of all traffic the security policy handles. Similarly, the `Content_Archive` sensor will save a full DLP archive of all traffic handled the security policy you apply it to. These two sensors are configured to detect all traffic of the supported types and archive them. You can see these sensors in the GUI but the configuration is only visible through the CLI; DLP archiving is set in the CLI only.

To set the archive to Summary

```
config dlp sensor
   edit <name of sensor>
      set summary-proto smtp pop3 imap http ftp nntp msn yahoo mapi
   end
```

To set the archive to Full

```
config dlp sensor
   edit <name of sensor>
      set full-archive-proto smtp pop3 imap http ftp nntp msn yahoo mapi
   end
```

If you set the `full-archive-proto` filter to include one or more of the protocols set by the `proto`option, then the archive action is disabled.

DLP examples

You can configure DLP sensors and filters when your FortiGate is operating in proxy-based inspection.

Blocking content with credit card numbers

When the objective is to block credit card numbers one of the important things to remember is that two filters will need to be used in the sensor. One filter is to prevent sensitive files from being leaked and another is to retain any sensitive data that is not a file (for example, messages or email content).

In the default Credit-Card sensor, you will notice a few things.

- The **Action** is set to **Log Only**
- In the **Files** filter not all of the services are being examined.

If you wish to block as much content as possible with credit card numbers in it instead of just logging most the traffic that has it, the existing sensor will have to be edited.

1. Go to **Security Profiles > Data Leak Prevention**.

Some configurations will have a preconfigured Credit Card sensor where you can use the drop down menu to select **Credit-Card**. If your configuration doesn't already have one create a new sensor.

2. Use the **Create New** icon to add a new sensor.
3. *Create/edit the first filter.* Set **Type** to **Messages** and select **Containing Credit Card #**.
4. Go to **Examine the Following Services** and select all services .
5. Set **Action** to **Block**.
6. Select **OK** or **Apply**.
7. *Create/edit the second filter.* Set **Type** to **Files** and select **Containing Credit Card #**.
8. Go to **Examine the Following Services** and select all services .
9. Set **Action** to **Block**.
10. Select **OK** or **Apply**.
11. Edit the appropriate policies so that under **Security Profiles**, **DLP** is turned on and the **Credit-Card** sensor is selected.

Blocking emails larger than 15 MB and logging emails from 5 MB to 15 MB

Multiple filters will have to be used in this case and the order that they are used is important. Because there is no mechanism to move the filters within the sensor the order that they are added to the sensor is important.

1. Go to **Security Profiles > Data Leak Prevention**.
2. Use the **Create New** icon to add a new sensor. Give it a descriptive **Name**, such as *block_large_emails*. Optionally, enter a descriptive comment.

Once the sensor has been created, a new filter will need to be added.

3. *Create the filter to block the emails over 15 MB*. In the filters table select **Create New**.
4. Set **Type** to **Messages** and enter 15360 in the field next to **File size over**. (1MB = 1024KB, 15 MB = 15 x 1024KB = 15360KB)
5. Go to **Examine the Following Services** and select all **Email** services .
6. Set **Action** to **Block**.
7. Select **OK**.

8. *Create the filter to log emails between 5 MB and 10 MB*. In the filters table select **Create New**.
9. Set **Type** to **Files**.
10. Enter 5120 in the field next to **File size over**. (1MB = 1024KB, 5 MB = 5 x 1024KB = 5124KB)
11. Go to **Examine the Following Services** and select all the email services .
12. Set action to **Log Only**.
13. Select **OK.**

The reason that the block filter is placed first is because the filters are applied in sequence and once the traffic triggers a filter, the action is applied and then the traffic is passed on to the next test. If the Log Only filter which checks for anything over 1MB is triggered this would include traffic over 15MB, so a 16 MB file would only be logged. In the described order, the 16 MB file will be blocked and the 3 MB file will be logged.

Blocking selectively based on a fingerprint

The following is a fairly complex example but shows what can be done by combining various components in the correct configuration.

The company has a number of copyrighted documents that it does not want “escaping” to the Internet but it does want to be able to send those documents to the printers for turning into hardcopy.

The policies and procedures regarding this issue state that:

- Only members of the group **Senior_Editors** can send copyrighted material to the printers.
- Every member of the company by default is included in the group **employees**.
- Even permitted transmission of copyrighted material should be recorded.
- All of the printers IP addresses are in a group called **approved_printers**.
- There is a file share called **copyrighted** where any file that is copyrighted is required to have a copy stored.
- It doesn’t happen often but for legal reasons sometimes these files can be changed, but all versions of a file in this directory need to be secured.
- All network connections to the Internet must have AntiVirus enabled using at least the default profile.
- The SSL/SSH Inspection profile used will be **default**.

It is assumed for the purposes of this example that:

- Any addresses or address groups have been created.
- User accounts and groups have been created.
- The account used by the FortiGate is fgtaccess.
- The copyrighted sensitivity level needs to be created.
- The copyrighted material is stored at \\192.168.27.50\books\copyrighted\

1. Add a new Sensitivity Level by running the following commands in the CLI:

```
config dlp fp-sensitivity
   edit copyrighted
end
```

2. Apply files to the fingerprint database by running these commands in the CLI:

```
config dlp fp-doc-source
   edit "copyrighted_material"
      set server-type smb
      set server 192.168.27.50
      set username fgtaccess
```

```
      set password ******
      set file-path books/copyrighted/
      set file-pattern *.pdf
      set sensitivity copyrighted
      set period daily
      set tod-hour 2
      set tod-min 0
      set scan-subdirectories enable
      set remove-deleted disable
      set keep-modified enable
   next
end
```

Two Sensors need to be created. One for blocking the transmission of copyrighted material and a second for allowing the passing of copyrighted material under specific circumstances.

3. Create the first DLP Sensor with the following commands in CLI:

```
config dlp sensor
   edit block_copyrighted
      config filter
         edit 1
            set proto smtp pop3 imap http-get http-post ftp nntp mapi
            set filter-by fingerprint
            set fp-sensitivity copyrighted
            set action block
         next
      end
   next
```

4. Create the second DLP Sensor

```
config dlp sensor
   edit allow_copyrighted
      config filter
         edit 2
            set proto smtp pop3 imap http-get http-post ftp nntp mapi
            set filter-by fingerprint
            set fp-sensitivity copyrighted
            set action log-only
         next
      end
   next
```

5. Create a policy to allow transmission of copyrighted material.
   a. Go to **Policy & Objects > IPv4 Policy**.
   b. Select **Create New**.
   c. Use the following values in the policy:

Incoming Interface	LAN
Source Address	all

Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	all
Action	ACCEPT
Enable NAT	enabled -- Use Destination Interface Address
AntiVirus	<ON> default
DLP	<ON> Copyrighted
SSL/SSH Inspection	<ON> default
Enable this policy	<ON>

This policy should be placed as close to the beginning of the list of policies so the it is among the first tested against.

6. Create a policy to block transmission of copyrighted material.
This will in effect be the default template for all following policies in that they will have to use the DLP profile that blocks the transmission of the copyrighted material.
   a. Go to **Policy & Objects > IPv4 Policy**.
   b. Select **Create New** or Edit an existing policy.
   c. Use the following values in the Policy:

   The fields should include what ever values you need to accomplish your requirements are but each policy should include the DLP sensor block_copyrighted. Alternatively, if a different DLP configuration is required it should include a filter that blocks **copyrighted** fingerprinted file.

   If you need to create a policy that is identity based make sure that there is an Authentication rule for the group **employees** that uses the DLP sensor that blocks copyrighted material.

ICAP support

ICAP is the acronym for Internet Content Adaptation Protocol. The purpose of the feature is to offload work that would normally take place on the firewall to a separate server specifically set up for the specialized processing of the incoming traffic. This takes some of the resource strain off of the FortiGate firewall leaving it to concentrate its resources on things that only it can do.

Offloading value-added services from Web servers to ICAP servers allows those same web servers to be scaled according to raw HTTP throughput versus having to handle these extra tasks.

ICAP servers are focused on a specific function, for example:

- Ad insertion
- Virus scanning
- Content translation
- HTTP header or URL manipulation
- Language translation
- Content filtering

The following topics are included in this section:

ICAP does not appear by default in the GUI. You must enable it in **System > Feature Visibility** .

The protocol

ICAP is an Application layer protocol; its specifications are set out in RFC 3507. It is, in essence, a lightweight protocol for executing a "remote procedure call" on HTTP messages and is a member of the member of the TCP/IP suite of protocols.

The default TCP that is assigned to it is 1344. Its purpose is to support HTTP content adaptation by providing simple object-based content vectoring for HTTP services. ICAP is usually used to implement virus scanning and content filters in transparent HTTP proxy caches. Content adaptation refers to performing the particular value added service, or content manipulation, for an associated client request/response.

Essentially it allows an ICAP client, in this case the FortiGate firewall, to pass HTTP messages to an ICAP server like a remote procedure call for the purposes of some sort of transformation or other processing adaptation. Once the ICAP server has finished processing the content, the modified content is sent back to the client.

The messages going back and forth between the client and server are typically HTTP requests or HTTP responses. While ICAP is a request/response protocol similar in semantics and usage to HTTP/1.1 it is not HTTP nor does it run over HTTP, as such it cannot be treated as if it were HTTP. For instance, ICAP messages can not be forwarded by HTTP surrogates.

Offloading using ICAP

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to an ICAP server in the ICAP profile added to the policy. Responses from the ICAP server are returned to the FortiGate unit which forwards them to an HTTP client or server.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers.

If the FortiGate unit supports HTTPS inspection, HTTPS traffic intercepted by a policy that includes an ICAP profile is also offloaded to the ICAP server in the same way as HTTP traffic.

When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Configuring ICAP

You will need to configure an ICAP server and an ICAP profile.

ICAP servers

1. Go to **Security Profiles > ICAP Servers** and click on **Create New**.
2. Enter a **Name** for the server.
3. Enter the server's **IP Address**. Depending on whether you've set the IP version to 4 or 6 will determine the format that the content of this field will be set into. In the GUI it looks like the same field with a different format but in the CLI it is actually 2 different fields named "ip-address" and ip6-address.
4. Set the **Port**; 1344 is default TCP port used for the ICAP traffic. The range can be from 1 to 65535.

Maximum Connections

This value refers to the maximum number of concurrent connections that can be made to the ICAP server. The default setting is 100. This setting can only be configured in the CLI.

The syntax is:

```
config icap server
   edit <icap_server_name>
      set max-connections <integer>
      end
```

Profiles

1. Go to **Security Profiles > ICAP** and click on **Create New**.
2. Enter a **Name** for the server.
3. Enable settings as required.

a. **Enable Request Processing** allows the ICAP server to process request messages. If enabled this setting will also require:

- **Server** - This is the name of the ICAP server. It is chosen from the drop down menu in the field. The servers are configure in the Security Profiles > ICAP > Server section.
- **Path** - This is the path on the server to the processing content. For instance if the Windows share name was “Processes” and the directory within the share was “Content-Filter” the path would be “/Processes/Content-Filter/”
- **On Failure** - There are 2 options: **Error** or **Bypass**.

b. **Enable Response Processing** allows the ICAP server to process response messages. If enabled this setting will also require:

- **Server** - This is the name of the ICAP server. It is chosen from the drop down menu in the field. The servers are configure in the Security Profiles > ICAP > Server section.
- **Path** - This is the path on the server to the processing compent. For instance if the Windows share name was “Processes” and the directory within the share was “Content-Filter” the path would be “/Processes/Content-Filter/”
- **On Failure** - There are 2 options. You can choose by the use of radio buttons either **Error** or **Bypass**.

c. **Enable Streaming Media Bypass** allows streaming media to ignore offloading to the ICAP server.

4. Select **Apply**.

Example ICAP sequence

This example is for an ICAP server performing web URL filtering on HTTP requests

1. A user opens a web browser and sends an HTTP request to connect to a web server.
2. The FortiGate unit intercepts the HTTP request and forwards it to an ICAP server.
3. The ICAP server receives the request and determines if the request is for URL that should be blocked or allowed.
   - If the URL should be blocked the ICAP server sends a response to the FortiGate unit. The FortiGate unit returns this response to the user’s web browser. This response could be a message informing the user that their request was blocked.
   - If the URL should be allowed the ICAP server sends a request to the FortiGate unit. The FortiGate unit forwards the request to the web server that the user originally attempted to connect to.
   - When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Example ICAP scenario

Information relavent to the following example:

- The ICAP server is designed to do proprietary content filtering specific to the organization so it will have to receive the messages and sent back appropriate responses.
- The content filter is a required security precaution so it if the message cannot be processed it is not allowed through.
- Resources on both the FortiGate and the ICAP server are considerable so the maximum connections setting will set at a double the default value to analyze the impact on performance.
- The ICAP server’s IP address is 172.16.100. 55.
- The path to the processing component is “/proprietary_code/content-filter/”.

- Streaming media is not something that the filter considers, but is allowed through the policy so processing it would be a waste of resources.
- The ICAP profile is to be added to an existing firewall policy.
- It is assumed that the display of the policies has already been configured to show the column “ID”.

1. Enter the following to configure the ICAP server:

   Go to **Security Profiles > ICAP Servers**.
   Use the following values:

Name	content-filtration-server4
IP Type	IPv4
IP Address	172.16.100.55
Port	1344

   Use the CLI to set the max-connections value.

```
config icap server
   edit content-filtration-server4
      set max-connections 200
      end
```

2. Enter the following to configure the ICAP profile to then apply to a security policy:

   Use the following values:

Name	Prop-Content-Filtration
Enable Request Processing	enable
Server	content-filtration-server4
Path	/proprietary_code/content-filter/
On Failure	Error
Enable Response Processing	enable
Server	content-filtration-server4
Path	/proprietary_code/content-filter/
On Failure	Error
Enable Streaming Media Bypass	enable

3. Apply the ICAP profile to policy:

The purposes of this particular ICAP profile is to filter the content of the traffic coming through the firewall via policy ID#17.

a. Go to **Policy & Objects > IPv4 Policy**.
b. Open the existing policy ID# 17 for editing.
c. Go to the section **Security Profiles.**
d. Select the button next to **ICAP** so that it indicates that it's status is **ON**.
e. Select the field with the profile name and use the drop down menu to select **Prop-Content-Filtration.**
f. Select **OK**.

FortiClient Compliance Profiles

This section describes the FortiClient Compliance Profiles endpoint protection features and configuration.

FortiClient Compliance Profiles are used primarily to make sure connected devices are compliant with Endpoint Control and to protect against vulnerabilities. Both **Endpoint Vulnerability Scan on Client** and **System compliance** are enabled by default, while other settings are disabled by default. This allows FortiClient to work as part of a Security Fabric.

FortiClient Profiles was renamed **FortiClient Compliance Profiles** to clarify that this profile only creates "compliance rules" and cannot be used to "provision FortiClient endpoints".

You must first enable this feature. Go to System > Feature Visibility and enable Endpoint Control. This will reveal the Security Profiles > FortiClient Compliance menu item.

The following topics are included in this section:

Endpoint protection overview

Endpoint Protection enforces the use of up-to-date FortiClient Endpoint Security software on endpoints (workstation computers and mobile devices). It pushes a FortiClient profile to the FortiClient application, specifying security settings, including:

- Real-time antivirus protection - on or off
- FortiClient web category filtering based on web filters defined in a FortiGate Web Filter profile
- FortiClient Application Control (application firewall) using application sensors defined in the FortiGate Application Control profile

The FortiClient profile can also:

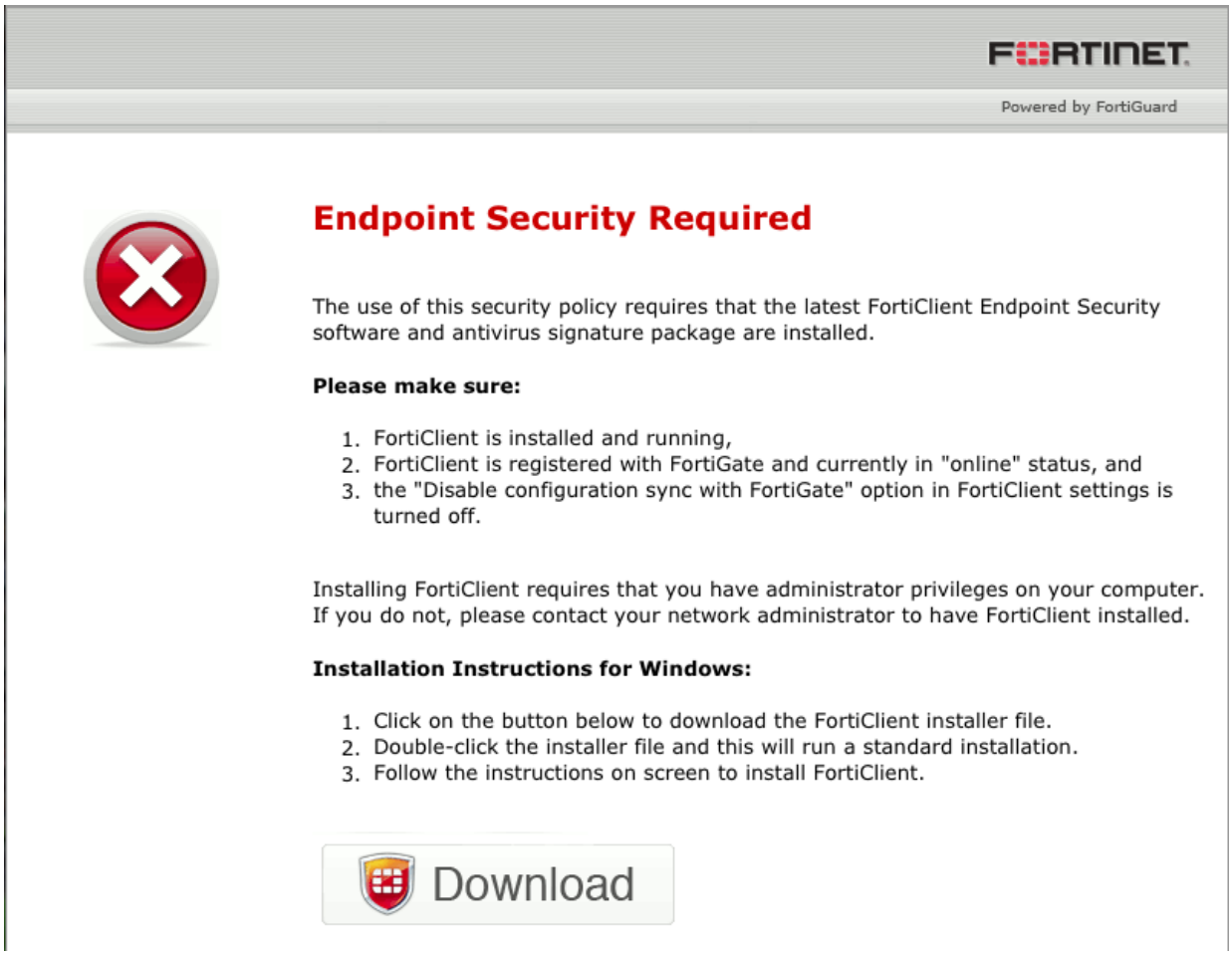
- Create VPN configurations
- Install CA certificates
- Upload logs to FortiAnalyzer or FortiManager
- Enable use of FortiManager for client software/signature update
- Enable a dashboard banner
- Enable client-based logging while on-net
- Output a mobile configuration profile (.mobileconfig file for iOS)

User experience

When using a web browser, the user of a non-compliant endpoint receives a replacement message HTML page from the FortiGate unit. The message explains that the user needs to install FortiClient Endpoint Security and provides a link to do so. The user cannot continue until the FortiClient software is installed.

For information about modifying the replacement message, see Modifying the endpoint protection replacement messages on page 196.

Default FortiClient non-compliance message for Windows



After installing FortiClient Endpoint Security, you will receive an invitation to register with the FortiGate unit. If you accept the invitation, the FortiClient profile is sent to the device's FortiClient application. Now the device is compliant and can connect to the network. FortiClient Endpoint Security registered with a FortiGate unit does not need to be separately licensed with FortiGuard.

The FortiGate unit can also register endpoints connecting over the Internet through a VPN. See Configuring endpoint registration over a VPN on page 192.

Licensing and FortiGate endpoint registration limits

To view the number of endpoints that are registered and the total that can be registered, go to **Dashboard**. Under **Licenses**, find **FortiClient**. You will see text like "4 /10". This means that there are four registered endpoints and a total of ten are allowed.

When the registration limit is reached, the next FortiClient-compatible device will not be able to register with the FortiGate unit. A message appears in the FortiClient application. The FortiClient profile is not sent to client and the client cannot connect through the FortiGate unit.

For all FortiGate models, the maximum number of registered endpoints is ten. For all models except 20C, you can purchase an endpoint license to increase this capacity:

To add an endpoint license - GUI

1. Go to **Dashboard**.
2. In the **Licenses** widget, click on **FortiClient**, select **Enter License**.
3. Enter the license key in the window that sllides in from the right, and select **OK**.

Maximum registered endpoints with endpoint license

FortiClient endpoint licenses for FortiOS 5.6.0 can be purchased in multiples of 100. There is a maximum client limit based on the FortiGate's model. FortiCare enforces the maximum limits when the customer is applying the license to a model.

If you are using the ten free licenses for FortiClient, support is provided on the Fortinet Forum (forum.fortinet.com). Phone support is only available for paid licenses.

Model(s)	Maximum client limit
VM00	200
FGT/FWF 30 to 90 series	200
FGT 100 to 400 series	600
FGT 500 to 900 series, VM01, VM02	2,000
FGT 1000 to 2900 series	20,000
FGT 3000 to 3600 series, VM04	50,000
FGT 3700D and above, VM08 and above	100,000

Older FortiClient SKUs will still be valid and can be applied to FortiOS 5.4 and 5.6.

Configuring endpoint protection

Endpoint Protection requires that all hosts connecting to an interface have the FortiClient Endpoint Security application installed. Make sure that all endpoints behind the interface are able to install this application. Currently, FortiClient Endpoint Security is available for Microsoft Windows (2000 and later), Apple (Mac OS X and later), and Android devices only.

By default, the FortiGuard service provides the FortiClient installer. If you prefer to host it on your own server, see Changing the FortiClient installer download location, below.

To set up Endpoint Protection, complete the following:

- Create a FortiClient Profile or use the default profile. See Creating a FortiClient profile on page 187. Enable the application sensor and web category filtering profiles that you want to use.
- Configure the FortiGate unit to support endpoint registration using FortiTelemetry (under **Network > Interfaces**, allow FortiTelemetry admission control).
- Optionally, enforce FortiClient registration. See Enforcing FortiClient registration on page 188.
- Optionally, configure application sensors and web filter profiles as needed to monitor or block applications.
- Optionally, modify the **Endpoint NAC Download Portal** replacement messages (one per platform). See Modifying the endpoint protection replacement messages on page 196.

Creating a FortiClient profile

FortiClient profiles allow you to perform vulnerability scans on endpoints and make sure endpoints are running compliant versions of FortiClient. Also, security posture features cause FortiClient to apply realtime protection, AntiVirus, web filtering, and application control on endpoints.

It is possible for more than one profile to be assigned to a device type. As with security policies, clients are matched to FortiClient profiles in the order that the profiles appear in the list.

Features involving general settings have been removed from the FortiClient profile GUI in 5.4.1. Features emphasizing compliance of the endpoint devices have been added. These enhancements facilitate integration with the Security Fabric.

To create a FortiClient profile - GUI

1. If you plan to use the Application Firewall feature in the FortiClient profile, go to **Security Profiles > Application Control** to create the Application Sensors that you will need.
2. If you plan to use the Web Category Filtering, go to **Security Profiles > Web Filter** to create the Web Filter Profile that you will need.
3. Go to **Security Profiles > FortiClient Compliance**. If there is only the default FortiClient profile, it will be displayed and ready to edit. At the top right of the page you can select or create other profiles.
4. Select **Create New** or edit an existing profile.
5. In **Assign Profile To**, select the device groups, user groups, and users to which this FortiClient profile applies. ***This is not available for the* default *profile.***
6. Set the **Endpoint Vulnerability Scan on Client** quarantine level. Similar to FortiOS 5.4, you can set the FortiClient Profile to run the FortiClient vulnerability scanner on endpoints and you can set the vulnerability quarantine level to quarantine endpoints that don't comply.The FortiGate will quarantine a host when a

vulnerability with the level of severity selected, or higher, is detected. Options are: **Critical**, **High**, **Medium**, **Low**, and **Information**.

7. **System Compliance**FortiOS 5.6 system compliance settings are similar to those in 5.4 with the addition of a non-compliance action. System compliance checking is performed by FortiClient but the non-compliance action is applied by the FortiGate:
   - select the **Minimum FortiClient version**, if necessary. The lowest supported version is 5.4.1.
   - identify which logs, if any, you will upload to FortiAnalyzer
   - set the **Non-compliance action**: **Block** or **Warning**.
8. Under **Security Posture Check**, enable the required options for your network:
   - **Realtime Protection**
   - **Third party AntiVirus on Windows** is required for Windows endpoints
   - identify which logs, if any, you will upload to FortiAnalyzer
   - select whether to enable an **Web Filter** security profile, and / or an**Application Control** sensor.
   - set the **Non-compliance action**: **Block** or **Warning**.
9. Select **OK** or **Apply**.

To create a FortiClient profile - CLI:

This example creates a profile for Windows and Mac computers.

```
config endpoint-control profile
   edit ep-profile1
      set device-groups mac windows-pc
      config forticlient-winmac-settings
         set forticlient-av enable
         set forticlient-wf enable
         set forticlient-wf-profile default
      end
   end
```

Support FortiClient for Linux

FortiClient for Linux (Ubuntu, CentOS, Red Hat, and Fedora) is also supported.

Syntax

```
config forticlient-winmac-settings
   config forticlient-operating-system
      edit <id>
         set os-type {ubuntu-linux | centos-linux | redhat-linux | fedora-linux | ...}
      next
   set forticlient-linux-ver <forticlient-version>
end
```

Enforcing FortiClient registration

When you enable FortiTelemetry (formerly known as FortiHeartbeat) on an interface, the option to enforce FortiClient registration becomes available. Devices connecting to that interface are forced to register to the FortiGate and install FortiClient before gaining access to network services.

The following example includes editing the default FortiClient Profile to enforce real time antivirus protection and malicious website blocking.

To enforce FortiClient registration on the internal interface - GUI:

1. On the FortiGate, go to **System > Feature Visibility** and enable **Endpoint Control**.
2. Go to **Network > Interfaces** and edit the internal interface.
3. Under **Administrative Access**, enable **FortiClient Telemetry**.
4. Under **Admission Control**, enable **Enforce FortiClient Compliance Check**.
   Once this is enabled, you have the option to **Exempt Sources** and/or **Exempt Destinations/Services**. If you were to exempt a source device, that device would not require FortiClient registration to access network services or the Internet.
5. Go to **Security Profiles > FortiClient Profiles**.
6. Under the **Security Posture Check** , enable **Realtime Protection**, **Up-to-date signatures**.

Endpoint compliance checking

Previously, as part of the Endpoint Compliance - Authorized Machine Detection feature, the administrator could specify a process name and SHA256 signature for a process, and only allow access to hosts with the specified process/application running. The FortiGate verifies if the process name and hash is matched on the connecting host to allow access.

In FortiOS 6.0, however, the FortiGate only matches the process name, and matching the SHA256 signature is optional (since the process may be updated dynamically and the signature may not match). The administrator can specify a process name and not specify a checksum, and so only the file name will be matched. If both file name and MD5 are specified, then both fields will still be matched.

A host check table has been added to the FortiClient Profile GUI, which is similar to a policy table; the match is performed from top to bottom. At the bottom of the table, there is an implicit entry, representing everything that does not match the higher entries. This implicit entry is always available, but the administrator can change the action to either **present** or **absent** (in reference to the specified process/application).

Syntax

A new attribute `application-check-rule` determines if the entry is for checking the presence or absence of an application:

```
config endpoint-control profile
   edit <name>
      config forticlient-winmac-settings
         ....
         config forticlient-running-app
            edit 1
               set app-name "MSOffice"
               set application-check-rule {present | absent}
               set process-name "word.exe"
            next
         ...
```

In addition, the `app-sha256-signature` entry is no longer mandatory, so long as the `process-name` entry is set:

```
config endpoint-control profile
```

```
edit <name>
   config forticlient-winmac-settings
   ....
      config forticlient-running-app
         edit <name>
            set app-name <name>
            set application-check-rule present
            set process-name "word.exe"
            set app-sha256-signature ''      <== this field can be left empty
            set process-name2 "excel.exe"
            set app-sha256-signature2 ''     <== not mandatory if process-name entry is set
            set process-name3 ''
            set app-sha256-signature3 ''     <== not mandatory if process-name entry is set
            set process-name4 ''
            set app-sha256-signature4 ''     <== not mandatory if process-name entry is set
         next
      ...
```

Enforcing FortiClient EMS requirements

FortiClient Compliance Profiles allow you to add up to three Enterprise Management Server (EMS) servers under **Security Profiles > FortiClient Compliance Profiles**.

This replaces the feature-related configuration (i.e AV, WF configuration) for compliance checks. Instead, if a FortiClient endpoint is managed by the defined EMS and is "in-sync" with the EMS profile then it is considered compliant.

An endpoint is considered compliant (thus allowed network access) only when the following conditions are met:

- the endpoint has FortiClient software
- the FortiClient software is managed by the authorized EMS server

Any endpoint that does not meet the above criteria (unless exempted) will be blocked from network access, regardless of FortiClient settings on that endpoint.

Syntax

```
config endpoint-control profile
   edit <name>
      config {forticlient-winmac-settings | forticlient-android-settings | forticlient-
          ios-settings}
         set forticlient-ems-compliance {enable | disable}
         set forticlient-ems-compliance-action {block | warning}
         set forticlient-ems-entries [addr1] [addr2] [addr3]
      next
   end
end

config endpoint-control settings
   set forticlient-ems-rest-api-call-timeout <milliseconds>
end
```

Changing the FortiClient installer download location

By default, FortiClient installers are downloaded from the FortiGuard network. You can also host these installers on a server for your users to download. In that case, you must configure FortiOS with this custom download location. For example, to set the download location to a customer web server with address custom.example.com, enter the following command:

```
config endpoint-control settings
   set download-location custom
   set download-custom-link "http://custom.example.com"
end
```

Storing FortiClient configuration files

Advanced FortiClient configuration files of up to 32k may be stored:

1. Enable the advanced FortiClient configuration option in the endpoint profile:

```
config endpoint-control profile
   edit "default"
      set forticlient-config-deployment enable
      set fct-advanced-cfg enable
      set fct-advanced-cfg-buffer "hello"
      set forticlient-license-timeout 1
      set netscan-discover-hosts enable
   next
end
```

2. Export the configuration from FortiClient (xml format).
3. Copy the contents of the configuration file and paste in the advanced FortiClient configuration box.

If the configure file is greater than 32k, you need to use the following CLI:

```
config endpoint-control profile
   edit <profile>
      config forticlient-winmac-settings
         config extra-buffer-entries
            edit <entry_id>
               set buffer xxxxxx
            next
         end
      end
   next
end
```

Blocking access to unsupported FortiClient endpoints

You can use the following command to deny registration of unsupported FortiClient endpoints. An unsupported FortiClient endpoint means the endpoint is running FortiClient but for some reason not all of the criteria are available to identify the endpoint, or the endpoint may be running an unsupported version of FortiClient. Information required that is not available could include the endpoint's IP address or MAC address is not visible.

```
config endpoint-control setting
   set forticlient-dereg-unsupported-client enable
end
```

Configuring the FortiClient offline grace period

Administrators can configure an offline grace period for registered and offline FortiClients so that PROBE can be processed and, as a result, endpoint compliance is not triggered.

- The grace period is allowed for a client that is compliant, registered, and offline.
- The grace period has a used status which determines if the client is before, during, or after grace period.
- Online and compliant clients will reset the grace status to unused.

Syntax

```
config endpoint-control settings
   set forticlient-offline-grace {enable | disable}
   set forticlient-offline-grace-interval <seconds>    <-- The default is 120
end
```

Configuring endpoint registration over a VPN

FortiGate units can register FortiClient-equipped endpoints over either an interface-based IPsec VPN or a tunnel-mode SSL VPN. After the user authenticates, the FortiGate unit sends the FortiClient application the IP address and port to be used for registration. If the user accepts the FortiGate invitation to register, registration proceeds and the FortiClient profile is downloaded to the client.

Users without FortiClient Endpoint Security connecting to the SSL VPN through a browser are redirected to a captive portal to download and install the FortiClient software.

Endpoint registration on an IPsec VPN

You can enable endpoint registration when you configure the FortiClient VPN or you can enable it on an existing FortiClient VPN.

To enable endpoint registration while configuring the VPN

- Enable **Allow Endpoint Registration** on the Policy & Routing page of the VPN Wizard when creating the FortiClient VPN.

This is only available when **Template Type** is set to **Remote Access** with a FortiClient **Remote Device Type**.

To enable endpoint registration on an existing VPN

1. Go to **Network > Interfaces** and edit the VPN's tunnel interface.
   The tunnel is a virtual interface under the physical network interface.
2. In **Admission Control**, enable **FortiClient Telemetry**.
   Optionally, you can also enable **Enforce FortiClient Telemetry for all FortiClients**. This forces endpoints to register with FortiClient before they have network access.
3. Select **OK**.

Endpoint registration on an SSL-VPN

To enable endpoint registration on the SSL-VPN

1. Go to **VPN > SSL-VPN Settings.**
2. In **Tunnel Mode Client Settings**, make sure **Allow Endpoint Registration** is enabled.
3. Select **Apply**.
4. Go to **Network > Interfaces** and edit the **ssl.root** interface.
5. In **Admission Control**, enable **FortiTelemetry**.
   Optionally, you can also enable **Enforce FortiClient Telemetry for all FortiClients**. This forces endpoints to register with FortiClient before they have network access.
6. Select **OK**.

This procedure does not include all settings needed to configure a working SSL-VPN.

Synchronizing endpoint registrations

To support roaming users in a network with multiple FortiGate units, you need to configure synchronization of the endpoint registration databases between the units. The registered endpoints are then recognized on all of the FortiGate units. This is configured in the CLI. For example, to synchronize this FortiGate unit's registered endpoint database with another unit named `other1` at IP address 172.20.120.4, enter:

```
config endpoint-control forticlient-registration-sync
   edit other1
      set peer-ip 172.20.120.4
   end
```

Assigning FortiClient Profiles using Microsoft AD user groups

When FortiClient Telemetry connects to FortiGate, the user's AD domain name and group are sent to FortiGate. Administrators may configure FortiGate to assign Endpoint Profiles based on the end user's AD domain group membership.

The following steps are discussed in more detail:

- Configuring users and groups on AD servers
- Configuring FortiAuthenticator
- Configuring FortiGate
- Connecting FortiClient Telemetry to FortiGate
- Monitoring FortiClient connections

Configuring users and groups on AD servers

Create the user accounts and groups on the AD server. Groups may have any number of users. A user may belong to more than one group at the same time.

Configuring FortiAuthenticator

Configure FortiAuthenticator to use the AD server you created. See the FortiAuthenticator Administration Guide in the Fortinet Document Library.

Configuring FortiGate

FortiGate

Add the FortiAuthenticator or Fortinet Single Sign-On Agent (FSSO):

1. Go to **Security Fabric > Fabric Connectors**.
2. Select **Create New** in the toolbar. The New Fabric Connector window opens.
3. Under **SSO/Identity**, select **Fortinet Single-Sign-On Agent**.
4. Enter the information required for the agent. This includes the name, primary and (optional) secondary IP addresses, and passwords. Select More FSSO agents to add up to three additional agents.
5. For **Collector Agent AD access mode**, select **Standard** or **Advanced**.
   a. **Standard**: select Users/Groups to include as Single-Sign-On accounts.
   b. **Advanced**: select an LDAP server in the dropdown list.
6. Select **OK** to save the agent configuration.

Create a user group:

1. Go to **User & Device > User Groups**.
2. Select **Create New** in the toolbar. The New User Group window opens.
3. In the **Type** field, select **Fortinet Single-Sign-On (FSSO)**.
4. Select members from the dropdown list.
5. Select **OK** to save the group configuration.

Configure the FortiClient profile:

1. Go to **Security Profiles > FortiClient Compliance**.
2. Select Create New in the toolbar. The New FortiClient Profile window opens.
3. Enter a profile name and optional comments.
4. In the **Assign Profile To** dropdown list select the FSSO user group(s).
5. Configure FortiClient configuration as required.
6. Select **OK** to save the new FortiClient profile.

Create any number of FortiClient profiles with different groups and different settings. The default profile will be assigned to users who connect successfully, but have no matching FortiClient profile.

Configure the firewall policy:

Configure the firewall policy. Ensure Compliant with FortiClient Profile is selected in the policy.

Connecting FortiClient Telemetry to FortiGate

The Microsoft Windows system where FortiClient is installed should join the domain of the AD server configured earlier. Users may log in with their domain username.

Following this, endpoint connections send the logged-in user's name and domain to the FortiGate. The FortiGate will assign the appropriate profiles based on the configurations.

Monitoring FortiClient connections

The following FortiOS CLI command lists information about connected clients. This includes domain-related details for the client if any.

```
diagnose endpoint record-list
   Record #1:
      IP_Address = 172.172.172.111(1)
      MAC_Address = b0:ac:6f:70:e0:a0
      Host MAC_Address = b0:ac:6f:70:e0:a0
      MAC list = b0-ac-6f-70-e0-a0;
      VDOM = root
      Registration status: Forticlient installed but not registered
      Online status: offline
      DHCP on-net status: off-net
      DHCP server: None
      FCC connection handle: 6
      FortiClient version: 5.1.29
      AVDB version: 22.137
      FortiClient app signature version: 3.0
      FortiClient vulnerability scan engine version: 1.258
      FortiClient feature version status: 0
      FortiClient UID: BE6B76C509DB4CF3A8CB942AED2064A0 (0)
      FortiClient config dirty: 1:1:1
      FortiClient KA interval dirty: 0
      FortiClient Full KA interval dirty: 0
      FortiClient server config: d9f86534f03fbed109676ee49f6cfc09::
      FortiClient config: 1
      FortiClient iOS server mconf:
      FortiClient iOS mconf:
      FortiClient iOS server ipsec_vpn mconf:
      FortiClient iOS ipsec_vpn mconf:
      Endpoint Profile: Documentation
      Reg record pos: 0
      Auth_AD_groups:
      Auth_group:
      Auth_user:
      Host_Name:
      OS_Version: Microsoft Windows 7 , 64-bit Service Pack 1 (build 7601)
      Host_Description: AT/AT COMPATIBLE
      Domain:
      Last_Login_User: FortiClient_User_Name
      Host_Model: Studio 1558
      Host_Manufacturer: Dell Inc.
      CPU_Model: Intel(R) Core(TM) i7 CPU Q 720 @ 1.60GHz
      Memory_Size: 6144
      Installed features: 55
      Enabled features: 21
```

```
online records: 0; offline records: 1
status -- none: 0; uninstalled: 0; unregistered: 1; registered: 0; blocked: 0
```

Modifying the endpoint protection replacement messages

If the security policy has **Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal** enabled, users of non-compliant devices are redirected to a captive portal that is defined by the **Endpoint NAC Download Portal** replacement message. There are different portals for Android, iOS, Mac, Windows, Quarantine, and “other” devices.

To modify the the endpoint protection replacement messages

1. Go to **System > Replacement Messages** and select **Extended View**.
2. In the **Endpoint Control** section select the message that you want to edit.
   The replacement message and its HTML code appear in a split screen in the lower half of the page.
3. Modify the text as needed and select **Save**.

Monitoring endpoints

Go to **Monitor > FortiClient Monitor** to monitor endpoints.

The **Monitor** page allows the user to view FortiClient endpoint devices grouped by interface and then sub-grouped by compliance status. Compliance status can be compliant, non-compliant, exempt, or quarantined.

Status	Enforcement Enabled	Enforcement Disabled
Compliant	List only active FortiClient endpoints.	No devices listed.
Not-compliant	List devices not-compliant with FortiClient profile, so long as they are not exempt.	No devices listed.
Exempt*	List FortiClient endpoints exempt from FortiClient compliance.	List of all user devices except those quarantined by the administrator.
Quarantined	List devices quarantined by the administrator.	List devices quarantined by the administrator.

* Includes device exempt reasons as any combination of device, device category/group, and source address.

You can see the reasons for non-compliance by right-clicking on an endpoint in the list.

Proxy options

Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out. When a security profile requiring the use of a proxy is enabled in a policy, the **Proxy Options** field is displayed. The Proxy Options define the parameters of how the traffic will be processed and to what level the traffic will be processed. There can be multiple security profiles of a single type. There can also be a number of unique Proxy Option profiles. As the requirements for a policy differ from one policy to the next, a different Proxy Option profile for each individual policy can be configured or one profile can be repeatedly applied.

The **Proxy Options** refer to the handling of the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- NNTP
- MAPI
- DNS

The configuration for each of these protocols is handled separately.

The use of different proxy profiles and profile options

Just like other components of the FortiGate, different Proxy Option profiles can be configured to allow for granular control of the FortiGate. In the case of the Proxy Option profiles the thing that you will want to focus on is the matching up of the correct profile to a firewall policy that is using the appropriate protocols. If you are creating a Proxy Option profile that is designed for policies that control SMTP traffic into your network you only want to configure the settings that apply to SMTP. You do not need or want to configure the HTTP components.

Proxy Options profile components

Highlighted below are certain features available in the **Proxy Options** security profile.

Log Oversized Files

This setting enables logging of the occurrence of oversized files being processed. It does not change how they are processed. It only enables the FortiGate unit to log that they were either blocked or allowed through. A common practice is to allow larger files through without antivirus processing. This allows you to get an idea of how often this happens and decide on whether or not to alter the settings relating to the treatment of oversized files.

The setting of the threshold for oversized files and emails is found on theSecurity Profiles > Proxy Options page under **Common Options**.

RPC over HTTP

FortiGate units with firmware version 5.4 and higher support RPC over HTTP. This protocol is used by the Microsoft Exchange Server to perform virus scanning of Microsoft Exchange Server email that uses RPC over HTTP. To enable this feature, go to **Security Profiles > Proxy Options** and enable **RPC over HTTP**.

Protocol Port Mapping

To optimize the resources of the unit, the mapping and inspection of protocols can be enabled or disabled.

Each of the protocols listed in the GUI has a commonly used default TCP port, however, the port used by the protocols can be individually modified. It can also be set to inspect any port with flowing traffic for that particular protocol. The headers of the packets indicate which protocol generated the packet.

Comfort Clients

When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit begins scanning the file. During the buffering and scanning procedure, the user must wait. After the scan is completed, if no infection is found, the file is sent to the next step in the process flow. If the file is a large one this part of the process can take some time. In some cases enough time that some users may get impatient and cancel the download.

The **Comfort Clients** feature mitigates this potential issue by feeding a trickle of data while waiting for the scan to complete. The user then knows that processing is taking place and that there hasn't been a failure in the transmission. The slow transfer rate continues until the antivirus scan is complete. Once the file has been successfully scanned and found to be clean of any viruses, the transfer will proceed at full speed.

If there is evidence of an infection, the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file. If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. A notification that the download has been blocked is displayed. The number of URLs in the cache is limited by the size of the cache.

Client comforting is available for HTTP and FTP traffic. If your FortiGate unit supports SSL content scanning and inspection, you can also configure client comforting for HTTPS and FTPS traffic.

Buffering the entire file allows the FortiGate unit to eliminate the danger of missing an infection due to fragmentation because the file is reassembled before examination. Client comforting can send unscanned and therefore potentially infected content to the client. You should only enable client comforting if you are prepared to accept this risk. Keeping the client comforting interval high and the amount low will reduce the amount of potentially infected data that is downloaded.

Block Oversized File/Email

This feature is related to antivirus scanning. The FortiGate unit has a finite amount of resources that can be used to buffer and scan a file. If a large file such as an ISO image or video file was to be downloaded this could overwhelm or exceed the memory of the FortiGate, especially if there were other large files being downloaded at the same time. For this reason, the treatment of large files needs to be addressed.

A threshold is assigned to identify an oversize file or email. This can be set at any size from 1 MB to 10 MB. Any file or email over this threshold will not be processed by policies applying the Antivirus security profile.

It should be noted that in terms of probability that malware is more likely to be found in smaller files than in larger files. A number of administrators take this into account when they lower the default threshold so as to lessen the impact on memory if they see the FortiGate unit going into conserve mode on a regular basis.

Chunked Bypass

The HTTP section allows the enabling of **Chunked Bypass**. This refers to the mechanism in version 1.1 of HTTP that allows a web server to start sending chunks of dynamically generated output in response to a request before actually knowing the actual size of the content. Where dynamically generated content is concerned, enabling this feature means that there is a faster initial response to HTTP requests. From a security stand point, enabling this feature means that the content will not be held in the proxy as an entire file before proceeding.

Allow Fragmented Messages

The specifications of RFC 2046 allow for the breaking up of emails and sending the fragments in parallel to be rebuilt and read at the other end by the mail server. It was originally designed to increase the performance over slower connections where larger email messages were involved. It will depend on your mail configuration if this is even possible for your network but outside of Microsoft Outlook and Outlook Express, not many email clients are set up to break up messages like this. The drawback of this feature is that if malware is broken up between multiple fragments of the message the risk is run that it will not be detected by some antivirus configurations because the code may not all be present at the same time to identify.

Append Email Signature

The **Append Email Signature** feature ensures that all of the emails going out of a particular network has the appropriate signature or corporate message, for example. These appended emails do not replace existing signatures.

Examples could include things like:

- Without prior approval the email should not be forwarded.
- Please be environmentally friendly and don’t print out emails
- For questions regarding the purchasing of our products please call…

It can be anything that the organization would like as long as it is in text format. The use of this feature usually works best in an environment where there is some standardization of what goes into the personal signatures of the senders so that there is no duplication or contradiction of information in the signatures.

SSL/SSH inspection

Individual deep inspection security profiles can be created depending on the requirements of the policy. Depending on the inspection profile selected, you can:

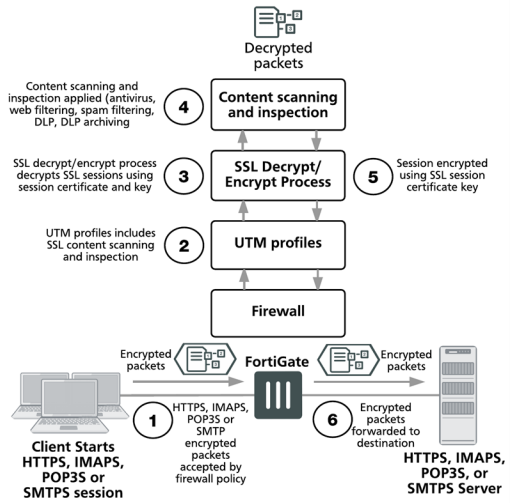
- Configure which Certificate Authority (CA) certificate will be used to decrypt the Secure Sockets Layer (SSL) encrypted traffic.
- Configure whether a specific SSL protocol will be inspected, blocked or bypassed.
- Configure which ports will be associated with which SSL protocols for the purpose of inspection.
- Configure which websites or website categories will be exempt from SSL inspection
- Identify how to treat invalid, unsupported or untrusted SSL certificates.
- Determine which inspection method will be applied to Secure Shell (SSH) / SSL traffic.

SSL inspection

Secure Sockets Layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:

- intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
- applies content inspection to decrypted content, including:
    - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
    - HTTPS web filtering and FortiGuard web filtering
    - IMAPS, POP3S, and SMTPS email filtering
- encrypts the sessions and forwards them to their destinations.

FortiGate SSL content scanning and inspection packet flow



SSL inspection and privacy

Normally, SSL decrypted content is temporarily stored in system memory for content scanning. If Malware is found the infected content is deleted and a message is sent to the destination instead. If no Malware is found the content is re-encrypted and forwarded to its destination. Administrators are not able to access or view the decrypted content.

There are two exceptions that you should be aware of if you have privacy concerns:

- If Sandbox inspection is enabled, either with an on-premises FortiSandbox device or FortiCloud Sandbox, decrypted files can be sent to FortiSandbox or FortiSandbox cloud where they can be viewed by system administrators.
- For flow-based SSL inspection, if SSL mirroring is enabled it is possible to "mirror" or send a copy of the decrypted content to one or more FortiGate interfaces so that the content can be collected by a raw packet capture tool for archiving or analysis. This feature is only available if the inspection mode is set to flow-based.

Decryption, storage, inspection, and use decrypted content is subject to local privacy rules. Use of these features could enable malicious users with administrative access to your FortiGate to harvest sensitive information submitted using an encrypted channel.

For increased privacy of sensitive information, you can use the SSL inspection exemptions feature, described below, to exempt sensitive communication from decryption.

SSL inspection exemptions

When you are using a browser to visit SSL encrypted sites and are using a certificate that does not match the certificate of the site, you are presented with a warning message and the option of continuing with the untrusted certificate, or terminating the session. However, there are a number of applications that use SSL encrypted traffic. Some applications will not allow SSL traffic that isn't signed with a trusted certificate. These applications do not necessarily give the option to manually indicate that we trust the certificate or the site. If the option is available, the customer may choose to import needed SSL certificates into Local Certificates and configure a policy for communication for that application.

To assist in preventing loss of access to these sites while still enabling the SSL inspection of the rest of the internet traffic, a method of exempting either web categories or specific sites has been developed. To exempt a large group of sites, the **SSL/SSH Inspection** profile can be configured to exempt FortiGuard Categories. There are three preselected categories due to the high likelihood of issues with associated applications with the type of websites included in these categories.

- Finance and Banking
- Heath and Wellness
- Personal Privacy

Other more specific websites can be added to the exemption list by going to **Security Profiles > SSL Inspection**, selecting the appropriate profile, and adding addresses under **Exempt from SSL Inspection**.

When you create a custom web category and tell the inspection profile to exempt that category, you may find some URLs in that category are still inspected. As a best practice, use the Static URL filter "Exempt" option instead.

Your FortiGate unit has two pre-configured SSL/SSH Inspection profiles that cannot be edited: **certificate-inspection** and **deep-inspection**. You must clone and edit the pre-configured profiles or create a new profile to exempt any additional sites or FortiGuard categories.

Allow Invalid SSL Certificates

It might seem like a straightforward decision that the allowing of invalid SSL certificates must be bad and, therefore, should not be allowed. However, there can be some reasons that applying this feature should be considered.

At a purely technical level, a properly formed certificate will encrypt the data so that it can only be read by the intended parties and not be read by anyone sniffing traffic on the network. For this reason, people will often use self-signed certificates. These self-signed certificates are free and will encrypt the data just as securely as a purchased certificate. The self-signed certificates, however, are not likely to recognized by the CA certificate store so will be considered by any checks against that store as invalid.

On the other hand, one of the services the vendors provide is verification of identity of those that purchase their certificates. This means that if you see a valid certificate from a site that identified itself as being from “valid-company.com” that you can be reasonably sure that the site does belong to that company and not a false site masquerading as being part of that company.

You can allow invalid SSL certificates by going to **Security Profiles > SSL Inspection**, selecting the appropriate profile, and enabling **Allow Invalid SSL Certificates**.

During the SSL handshake, a number of checks are made to verify the validity of the certificate.

One source of the checks, is against a CA certificate store inside FortiOS. This is the same CA bundle used by the browser Mozilla Firefox.

Updates to the store are:

- With each new version of FortiOS
- Via internal FGD
- Possible with some builds via FTP

Details of the CA certificate store can be found at: https://curl.haxx.se/docs/caextract.html

The following checks are made for validity:

Validity Check	Description
Signature	One of the things being checked against the CA bundle is the certificate signature. These signatures are generated via directly signing by the CA's private key.
Expiration date	All certificates have an expiry date. The date, based on the devices clock/calendar is compared to the expiry date of the certificate.
Revoked list	Periodically, certificates are revoked. If a certificate has been revoked it is put on a list. Whenever a certificate is being verified, it is checked against this list.

Validity Check	Description
Self signed certificate	In the case of self-signed certificates, the IPS engine and proxy have different handling. IPS engine will keep and use the certificate self-signed certificate, but the public key will be replaced so that SSL inspection can take place. The proxy engine will re-sign the certificate with the untrusted CA certificate. The mechanics are similar but the net effect for the user is similar. The user will get warnings from browsers. The users can choose to remember the self-signed certificate in some browsers, but cannot do the same thing with the certificate re-signed with the untrusted CA.
Intermediate CA with a weak hash algorithm, such as MD5, SHA1	Some browsers like Chrome or Firefox will give a warning because of a weak signature algorithm (visit https://sha1-intermediate.badssl.com to test). In the IPS Engine, in order to convey the weak intermediate CA back to client, the signature hash algorithm is downgraded in the re-signed server certificate to the weakest algorithm used in the original certificate chain. In the Proxy Engine - In the case of a weak signature algorithm, the Proxy engine will treat the connection as untrusted, and re-sign the server certificate with the untrusted CA. The final user experience is different. Instead of a warning like "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" that you would get in Chrome, you will get a warning that the certificate couldn't be verified (because of the signing CA is not trusted or imported into the user's web browser).

Flow-based behaviour

In flow-based mode, a certificate will be considered as **invalid** if it has expired.

In addition, a certificate will be considered as **untrusted** if one or more of the following conditions are met:

- If the chain is broken or incomplete.
- If it is part of the CRL.
- If the CA certificate was not imported to the FortiGate, or it is not in the FortiGate CA certificate store.

Why use SSL inspection

Most of us are familiar with Hypertext Transfer Protocol Secure (HTTPS) and how it protects a variety of activities on the Internet by applying Secure Sockets Layer (SSL) encryption to the web traffic. However, there are risks associated with its use, since encrypted traffic can be used to get around your network's normal defenses.

For example, you might download a file containing a virus during an e-commerce session. Or you could receive a phishing email containing a seemingly harmless downloader file that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer. Because the sessions in these attacks are encrypted, they might get past your network's security measures.

To protect your network from these threats, SSL inspection is the key your FortiGate uses to unlock encrypted sessions, see into encrypted packets, find threats, and block them. SSL inspection not only protects you from attacks that use HTTPS, but also from other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

Full SSL inspection

To make sure that all SSL encrypted content is inspected, you must use full SSL inspection (also known as deep inspection). When full SSL inspection is used, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the sender.

When the FortiGate re-encrypts the content it uses a certificate stored on the FortiGate. The client must trust this certificate to avoid certificate errors. Whether or not this trust exists depends on the client, which can be the computer's OS, a browser, or some other application, which will likely maintain it's own certificate repository. For more information about this, see the recipe Preventing certificate warnings on the Fortinet Cookbook site.

There are two deployment methods for full SSL inspection:

1. Multiple Clients Connecting to Multiple Servers:

- Uses a CA certificate (which can be uploaded using the **Certificates** menu).
- Typically applied to outbound policies where destinations are unknown (i.e. normal web traffic).
- Address and web category whitelists can be configured to bypass SSL inspection.

2. Protecting SSL Server

- Uses a server certificate (which can be uploaded using the **Certificates** menu) to protect a single server.
- Typically used on inbound policies to protect servers available externally through Virtual IPs
- Since this is typically deployed "outside-in" (clients on the Internet accessing server(s) on the internal side of the FortiGate), server certificates using the public FQDN of the server are often purchased from a commercial Certificate Authority and uploaded to the FortiGate. This avoids client applications generating SSL certificate errors due to certificate mismatch.

More detail is available in the Fortinet Knowledge Base. Check these technical notes:

- How to Enable SSL inspection from the CLI and Apply it to a Policy
- How to block web-based chat on Gmail webmail using App Sensor + SSL inspection

SSL certificate inspection

FortiGates also supports a second type of SSL inspection, called SSL certificate inspection. When certificate inspection is used, the FortiGate only inspects the header information of the packets.

Certificate inspection is used to verify the identity of web servers and can be used to make sure that HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. However, since only the packet is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

Troubleshooting

The most common problem with SSL inspection is users receiving SSL errors when the CA certificate is not trusted. This is because by default the FortiGate uses a certificate that is not trusted by the client. There are two

ways to fix this:

1. All users must import the FortiGate's default certificate into their client applications as a trusted certificate.
2. Configure the FortiGate to use a certificate that is already trusted by your clients. For example, a certification signed by a CA that your clients already trust.

The first method can be more labor intensive because you have to distribute a certification to all clients. This can also be an ongoing problem as new clients are added to your network. The second method is usually less work but may require paying for a CA. Both of these methods are covered in the recipe Preventing Certificate Warnings.

If you choose to install the certificate on client applications, this can be done with greater ease in a Microsoft Active Directory domain environment by using Group Policy Objects to install the certificate on domain members. Check that the Group Policy has propagated to all computers by opening Internet Explorer on a workstation PC, opening **Tools > Internet Options > Content > Certificates >Trusted Root Certification Authorities**, and ensuring that the FortiGate's certificate is present.

For corporate-owned mobile devices, MDM solutions like AirWatch, MobileIron, or Fiberlink, use Simple Certificate Enrollment Protocol (SCEP) to ease certificate enrollment.

Best practices

Because all traffic needs to be decrypted, inspected, and re-encrypted, using SSL inspection can reduce overall performance of your FortiGate. To make sure you aren't using too many resources for SSL inspection, do the following:

- **Know your traffic** – Know how much traffic is expected and what percent of the traffic is encrypted. You can also limit the number of policies that allow encrypted traffic.
- **Be selective** – Use white lists or trim your policy to apply SSL inspection only where it is needed.
- **Use hardware acceleration** - FortiGate models with either the CP6 or CPU processor have an SSL/TLS protocol processor for SSL content scanning and SSL acceleration. For more information about this, see the Hardware Acceleration handbook.
- **Test real-world SSL inspection performance yourself** - Use the flexibility of FortiGate's security policy to gradually deploy SSL inspection, rather than enabling it all at once.

Creating or editing an SSL/SSH Inspection profile

1. Go to **Security Profiles > SSL/SSH Inspection**. This will open to one of the existing profiles. Your FortiGate unit has two pre-configured SSL/SSH Inspection profiles that cannot be edited: certificate-inspection and deep-inspection. You must clone and edit the pre-configured profiles or create a new profile to exempt any additional sites or FortiGuard categories. The links for the actions are located in the upper right hand corner of the window.
   - To view a list of the existing profiles select the List icon (a page) at the far right.
   - To clone an existing profile, select the Clone icon (one page behind another), second from the right
   - To create a new profile, select the Create New icon ("+ "symbol), third from the right.
   - To view or edit an existing profile, choose it from the dropdown menu field.
2. **Name Field:**
   Give the profile an easily identifiable name that references its intent.

3. **Comments Field:**
   Enter any additional information that might be needed by administrators, as a reminder of the profile's purpose and scope.
4. **SSL Inspection Options:**
   a. Enable SSL Inspection of:
   - Multiple Clients Connecting to Multiple Servers - Use this option for generic policies where the destination is unknown.
   - Protecting SSL Server - Use this option when setting up a profile customized for a specific SSL server with a specific certificate.

   b. Inspection Method
   The options here are:
   - SSL Certificate Inspection - only inspects the certificate, not the contents of the traffic.
   - Full SSL Inspection - inspects all of the traffic.

   c. CA Certificate
   Use the drop down menu to choose which one of the installed certificates to use for the inspection of the packets or click on **Download Certificate.**

   d. Untrusted SSL Certificates
   Select an action for untrusted SSL certificates.

   d. **Protocol Port Mapping** / Inspect All Ports
   Enable the ability to inspect all ports by checking the box. If the feature is not enabled, specify in the field next to the listed protocols, the port through which that protocols traffic will be inspected. Traffic of that protocol going through any other port will not be inspected.

If you select **Inspect All Ports**, then only the IPS engine is used for inspection.

5. **Exempt from SSL Inspection**:
   Use the dropdown menus in this section to specify any reputable websites, FortiGuard Web Categories, or addresses will be exempt from SSL inspection.
   - Reputable Websites - Enable this option to exempt any websites identified by FortiGuard as reputable.
   - Web Categories - By default the categories of Finance and Banking, Health and Wellness, and Personal Privacy, have been added as these are one that are most likely to have applications that will require a specific certificate.
   - Addresses - These can be any of the Address objects that have an interface of "Any".
   - Log SSL exemptions - Enable this option to log all SSL exemptions
6. **SSH Inspection Options:**
   a. **SSH Deep Scan**
   Toggle to disable or enable the feature

   b. **SSH Port**
   The available options are:
   - **Any** - choosing this option will search all of the traffic regardless of service or TCP/IP port for packets that conform to the SSH protocol

- **Specify** - choosing this option will restrict the search for SSH protocol packets to the TCP/IP port number specified in the field. This is not as comprehensive but it is easier on the performance of the firewall.

d. Protocol Actions

- Exec - Block, Log or neither. Select using check boxes.
- Port-Forward - Block, Log or neither. Select using check boxes.
- SSH-Shell - Block, Log or neither. Select using check boxes.
- X11-Filter - Block, Log or neither. Select using check boxes.

6. **Common Options:**

a. Allow Invalid SSL Certificates
Check the box to enable the passing of traffic with invalid certificate

b. Log SSL anomalies
Check the box to allow the Logging function to record traffic sessions containing invalid certificates

The **Full SSL Inspection** method is enabled by default when creating a new SSL/SSH Inspection profile. There are situations were this feature can cause issues so be sure that you would like it enabled before applying the inspection profile.

Secure white list database

You can enable a feature that gathers a list of reputable domain names that can be excluded from SSL deep inspection. This list is periodically updated and downloaded to FortiGate units through FortiGuard.

Go to **Security Profiles > SSL Inspection**, enable **Exempt from SSL Inspection**, and enable **Reputable Websites**.The reputable websites are rated by FortiGuard. Web Filtering.

CLI syntax:

```
config firewall ssl-ssh-profile
   edit deep-inspection
      set whitelist enable
   end
end
```

SSH MITM deep inspection

As vulnerabilities of OpenSSH continue to be exposed, it has become necessary to detect such attacks, which requires the ability to decrypt the SSH tunnel to check the data. This feature introduces comprehensive security controls on SSH Man-in-the-Middle (MITM) deep inspections, including:

- SSH filter profiles to control SSH tunnel types and filtering on SSH shell commands.
- SSH proxy policies to apply a proxy firewall policy with user authentication on SSH session.
- Support for SSH tunnel policy to perform access control for TCP/IP port forwarding traffic that is tunneled through the SSH proxy. IPS scanning can be applied to the tunneled traffic.
- Support for SSH trust to detect and prevent SSH MITM attacks.

Syntax

1. Add SSH related option in ssl-ssh-profile for proxy mode profile

   a. Add option to bypass or block unsupported SSH protocol (Deep scan only supports SSH 2.0)

```
config firewall ssl-ssh-profile
   edit <name>
      config ssh
         set unsupported-version {bypass | block}
      next
   end
end
```

   b. Add option to enable SSH proxy policy check

```
config firewall ssl-ssh-profile
   edit <name>
      config ssh
         set ssh-policy-check {enable | disable}
         set ssh-tun-policy-check {enable | disable}
      next
   end
end
```

When SSH proxy policy check is enabled, proxy will check "SSH proxy" policy for SSH traffic and check "SSH tunnel" policy for TCP/IP port forwarding traffic.

   c. Move block/log options for `x11-filter/ssh-shell/exec/port-forward` to SSH filter profile

2. SSH filter profile

   a. Support options to block or log `x11-filter/ssh-shell/exec/port-forward/sftp`

```
config ssh-filter profile
   edit <name>
      set block {x11-filter | ssh-shell | exec | port-forward | sftp}
      set log {x11-filter | ssh-shell | exec | port-forward | sftp}
   next
end
```

   b. Add Shell command filters

```
config ssh-filter profile
   edit <name>
      config shell-commands
         edit <id>
            set type {simple | regex}
            set pattern <cmd-string>
            set action {block | allow}
            set log {enable | disable}
            set alert {enable | disable}
            set severity {low | medium | high | critical}
         next
      end
   set default-command-log {enable | disable}
end
```

3. Allow SSH filter profile to be set for `config firewall policy` when UTM is enabled.
4. Support SSH proxy policy for SSH sessions

   a. Add a proxy type `ssh` into `config firewall proxy-policy`

```
config firewall proxy-policy
   edit <pol-id>
      set proxy ssh
   next
end
```

   b. When `user`/`user-group` is set in SSH proxy policy, firewall authentication can be done for SSH proxy traffic. Authentication rule for SSH is added:

```
config authentication rule
   edit <name>
      set protocol ssh
   next
end
```

   i. "Basic" authentication scheme:

```
config authentication scheme
   edit "ssh-active"
      set method basic
      set user-database "local" #or LDAP server
   next
```

   ii. "ssh-publickey" authentication scheme:

```
config authentication scheme
   edit "ssh-pkey"
      set method ssh-publickey
      set user-database "local" #or LDAP server
      set ssh-ca "server-ca"
   next
```

   User name is embedded in ssh-publickey. User group information will be retrieved if the publickey is validated by CA.

   iii. Both "Basic" and "ssh-publickey" authentication scheme:

```
config authentication scheme
   edit "ssh-pkey"
      set method basic ssh-publickey
      set user-database "local" #or LDAP server
      set ssh-ca "server-ca"
   next
```

5. Support SSH tunnel policy to do access control for TCP/IP port forwarding traffic.

   a. Add a proxy type `ssh-tunnel` into `config firewall proxy-policy`

```
config firewall proxy-policy
   edit <pol-id>
      set proxy ssh-tunnel
      set action {accept | deny}
   next
end
```

   b. Support allow or deny and IPS sensor/app-control the traffic.

6. Support SSH trust to detect and prevent from SSH MITM attacks

a. Define trusted SSH hostkey for specific SSH server

```
config firewall ssh host-key
   edit <name>
      set status {trusted | revoked}
      set type {RSA | DSS | ECDSA}
      set nid <NID of ECDSA key>
      set ip <ip>
      set port <port>
      set hostname <name>
      set public-key <hostkey>
   next
end
```

b. Define trusted/untrusted CAs for hostkey signing. Any hostkey signed by trust CA is trusted unless the hostkey is revoked.

```
config firewall ssh local-ca
   edit <name>
      set password <passwd>
      set public-key <public key>
      set private-key <private key>
      set source {build-in | user}
   next
end
```

The system creates two build-in SSH CAs: Fortinet_SSH_CA and Fortinet_SSH_CA_Untrusted. The CAs are used to re-sign a server host key with local host-key using trusted/untrusted CA when the server host key is trusted or untrusted.

c. Define local hostkey templates for trusted re-signing. Be default, they are generated automatically.

```
config firewall ssh local-key
   edit <name>
      set password <passwd>
      set public-key <public key>
      set private-key <private key>
      set source {build-in | user}
   next
end
```

i. The system creates different types of local host keys as default re-signing templates: Fortinet_SSH_RSA2048, Fortinet_SSH_DSA1024, Fortinet_SSH_ECDSA256, Fortinet_SSH_ECDSA384, Fortinet_SSH_ECDSA512, Fortinet_SSH_ED25519, Fortinet_SSH_RSA1024.

ii. Admin can load their own local host keys and use them for MITM re-signing in `config firewall ssh setting`.

d. Per-VDOM SSH settings

```
config firewall ssh setting
   set caname <trusted-ca>
   set untrusted-caname <untrusted-ca>
   set hostkey-rsa <hostkey-rsa>
   set hostkey-dss <hostkey-dss>
   set hostkey-ecdsa256 <hostkey-ecdsa256>
```

```
   set hostkey-ecdsa384 <hostkey-ecdsa384>
   set ed25519-key <ed25519-key>
   set host-trusted-check {enable | disble}
end
```

i. When a hostkey is trusted and signed by a CA, SSH proxy re-signs appropriate type of hostkey using trusted CA.
ii. When a host is trusted but not signed, SSH proxy sends back appropriate type of hostkey.
iii. When a hostkey is untrusted and signed by a CA, SSH proxy re-signs a temporary hostkey (1 hour life time) using untrused CA.
iv. When a host is trusted but not signed, SSH proxy sends back a temporary hostkey (one hour life time).

SSL server table for SSL offloading

An SSL server table can now be used for SSL offloading. This feature was introduced with the release of FortiOS 5.4.0.

CLI Syntax

```
config firewall ssl-ssh-profile
   edit <name>
      set use-ssl-server {enable|disable}
   next
end
```

Custom Application & IPS Signatures

Creating a custom IPS signature

The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can add or edit custom signatures using the GUI or the CLI.

To create a custom signature

1. Go to **Security Profiles > Intrusion Prevention**.
2. Select **[View IPS Signatures]**
3. Select **Create New** to add a new custom signature.
4. Enter a **Name** for the custom signature.
5. Enter the **Signature**. For information about completing this field, see Custom signature syntax and Custom signature keywords.
6. Select **OK**.

Custom signature syntax

All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)

You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to **Security Profiles > Intrusion Prevention,** select **View IPS Signatures**, select **Create New**, and enter the data directly into the **Signature** field, following the guidance in the next topics.

The table below shows the valid characters and basic structure. For details about each keyword and its associated values, see Custom signature keywords.

Valid syntax for custom signature fields

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.

Field	Valid Characters	Usage
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Custom signature keywords

Information keywords

attack_id

Syntax: `--attack_id <id_int>;`

Description:

Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiGate automatically assigns an attack ID to the signature. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs.

An attack ID you assign must be between 1000 and 9999.

Example: `--attack_id 1234;`

name

Syntax: `--name <name_str>;`

Description:

Enter the name of the rule. A rule name must be unique. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same rule name for signatures in different VDOMs. The name you assign must be a string greater than 0 and less than 64 characters in length.

Example: `--name "Buffer_Overflow";`

Session keywords

flow

Syntax: `--flow {from_client[,reversed] | from_server[,reversed] | bi_direction };`

Description:

Specify the traffic direction and state to be inspected. They can be used for all IP traffic.

Example: `--src_port 41523; --flow bi_direction;`

The signature checks traffic to and from port 41523.

If you enable “quarantine attacker”, the optional reversed keyword allows you to change the side of the connection to be quarantined when the signature is detected.

For example, a custom signature written to detect a brute-force log in attack is triggered when “Login Failed” is detected from_server more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker.

Previous FortiOS versions used to_client and to_server values. These are now deprecated, but still function for backwards compatibility.

service

Syntax: `--service {HTTP | TELNET | FTP | DNS | SMTP | POP3 | IMAP | SNMP | RADIUS | LDAP | MSSQL | RPC | SIP | H323 | NBSS | DCERPC | SSH | SSL};`

Description:

Specify the protocol type to be inspected. This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content.

app_cat

Syntax: `--app_cat <category_int>;`

Description:

Specify the category of the application signature. Signatures with this keyword are considered as application rules. These signatures will appear under Application Control instead of IPS configuration. To display a complete list of application signature categories, enter the following CLI commands:

```
config application list
   edit default
      config entries
         edit 1
            set category ?
```

weight

Syntax: `--weight <weight_int>;`

Description:

Specify the weight to be assigned to the signature. This keyword allows a signature with the higher weight to have priority over a signature with a lower weight. This is useful to prioritize between custom and stock signatures and also between different custom signatures.

The weight must be between 0 an 255. Most of the signatures in the Application Control signature database have weights of 10; botnet signatures are set to 250. A range of 20 to 50 is recommended for custom signatures.

Content keywords

byte_extract

Syntax: `byte_extract:<bytes_to_extract>, <offset>, <name> \ [, relative][, multiplier <multiplier value>][, <endian>]\ [, string][, hex][, dec][, oct][, align <align value>][, dce];`

Description:

Use the `byte_extract` option to write rules against length-encoded protocols. This reads some of the bytes from the packet payload and saves it to a variable.

byte_jump

Syntax: `--byte_jump <bytes_to_convert>, <offset>[, multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct] [, align];`

Description:

Use the `byte_jump` option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to examine from the packet.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.

- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.
- `align`: Round up the number of converted bytes to the next 32-bit boundary.

byte_test

Syntax: `--byte_test <bytes_to_convert>, <operator>, <value>, <offset> [multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct];`

Description:

Use the `byte_test` keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to compare.
- `<operator>`: The operation to perform when comparing the value (<,>,=,!,&).
- `<value>`: The value to compare the converted value against.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.

depth

Syntax: `--depth <depth_int>;`

Description:

Use the depth keyword to search for the contents within the specified number of bytes after the starting point defined by the offset keyword. If no offset is specified, the offset is assumed to be equal to 0.

If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched.

The depth must be between 0 and 65535.

distance

Syntax: `--distance <dist_int>;`

Description:

Use the distance keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the within keyword is not specified, continue looking for a match until the end of the payload.

The distance must be between 0 and 65535.

content

Syntax: `--content [!]"<content_str>";`

Description:

Deprecated, see pattern and context keywords. Use the content keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.

To have the FortiGate search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.

Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character.

The double quote ("), pipe sign(|) and colon(:) characters must be escaped using a back slash if specified in a content string.

If the value of the content keyword is greater than the length of the value of the depth keyword, this signature will never be matched.

context

Syntax: `--context {uri | header | body | host};`

Description:

Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiGate unit searches for the pattern anywhere in the packet buffer. The available context variables are:

- `uri`: Search for the pattern in the HTTP URI line.
- `header`: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages.
- `body`: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body.
- `host`: Search for the pattern in HTTP HOST line.

no_case

Syntax: `--no_case;`

Description:

Use the no-case keyword to force the FortiGate unit to perform a case-insensitive pattern match.

offset

Syntax: `--offset <offset_int>;`

Description:

Use the offset keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the offset keyword with the depth keyword to stop looking for a match after a specified number of bytes. If no depth is specified, the FortiGate unit continues looking for a match until the end of the payload.

The offset must be between 0 and 65535.

pattern

Syntax: `--pattern [!]"<pattern_str>";`

Description:

The FortiGate unit will search for the specified pattern. A pattern keyword normally is followed by a context keyword to define where to look for the pattern in the packet. If a context keyword is not present, the FortiGate unit looks for the pattern anywhere in the packet buffer. To have the FortiGate search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.

Example: `--pattern "/level/" --pattern "|E8 D9FF FFFF|/bin/sh" --pattern !"|20|RTSP/"`

pcre

Syntax: `--pcre [!]"/<regex>/[ismxAEGRUB]";`

Description:

Similarly to the pattern keyword, use the pcre keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A pcre keyword can be followed by a context keyword to define where to look for the pattern in the packet. If no context keyword is present, the FortiGate unit looks for the pattern anywhere in the packet buffer.

For more information about PCRE syntax, go to http://www.pcre.org.

The switches include:

- `i`: Case insensitive.
- `s`: Include newlines in the dot metacharacter.
- `m`: By default, the string is treated as one big line of characters. ^ and $ match at the beginning and ending of the string. When m is set, ^ and $ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.
- `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.
- `A`: The pattern must match only at the start of the buffer (same as ^).
- `E`: Set $ to match only at the end of the subject string. Without E, $ also matches immediately before the final character if it is a newline (but not before any other newlines).
- `G`: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by ?.
- `R`: Match relative to the end of the last pattern match. (Similar to distance:0;).
- `U`: Deprecated, see the context keyword. Match the decoded URI buffers.

uri

Syntax: `--uri [!]"<uri_str>";`

Description:

Deprecated, see pattern and context keywords. Use the uri keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("). To have the FortiGate unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign (|) and colon (:) characters must be escaped using a back slash (\) if specified in a URI string.

within

Syntax: `--within <within_int>;`

Description:

Use this together with the distance keyword to search for the contents within the specified number of bytes of the payload.

The within value must be between 0 and 65535.

IP header keywords

dst_addr

Syntax: `--dst_addr [!]<ipv4>;`

Description:

Use the dst_addr keyword to search for the destination IP address. To have the FortiGate search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `dst_addr [172.20.0.0/16, 10.1.0.0/16,192.168.0.0/16]`

ip_dscp

Syntax: `--ip_dscp`

Description:

Use the ip_dscp keyword to check the IP DSCP field for the specified value.

ip_id

Syntax: `--ip_id <field_int>;`

Description:

Check the IP ID field for the specified value.

ip_option

Syntax: `--ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any};`

Description:

Use the ip_option keyword to check various IP option settings.

The available options include:

- `rr`: Check if IP RR (record route) option is present.
- `eol`: Check if IP EOL (end of list) option is present.
- `nop`: Check if IP NOP (no op) option is present.
- `ts`: Check if IP TS (time stamp) option is present.
- `sec`: Check if IP SEC (IP security) option is present.
- `lsrr`: Check if IP LSRR (loose source routing) option is present.
- `ssrr`: Check if IP SSRR (strict source routing) option is present.
- `satid`: Check if IP SATID (stream identifier) option is present.
- `any`: Check if IP any option is present.

ip_tos

Syntax: `--ip_tos <field_int>;`

Description:

Check the IP TOS field for the specified value.

ip_ttl

Syntax: `--ip_ttl [< | >] <ttl_int>;`

Description:

Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol.

protocol

Syntax: `--protocol {<protocol_int> | tcp | udp | icmp};`

Description:

Check the IP protocol header.

Example: `--protocol tcp;`

src_addr

Syntax: `--src_addr [!]<ipv4>;`

Description:

Use the src_addr keyword to search for the source IP address. To have the FortiGate unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `src_addr 192.168.13.0/24`

TCP header keywords

ack

Syntax: `--ack <ack_int>;`

Description:

Check for the specified TCP acknowledge number.

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the `dst_port` keyword to specify the destination port number.

You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

seq

Syntax: `--seq [operator,]<number>[,relative];`

Description:

Check for the specified TCP sequence number.

- `operator` includes =,<,>,!.
- `relative` indicates it's relative to the initial sequence number of the TCP session.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Use the src_port keyword to specify the source port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

tcp_flags

Syntax: `--tcp_flags <SAFRUP120>[!|*|+] [,<SAFRUP120>];`

Description:

Specify the TCP flags to match in a packet.

- `S`: Match the SYN flag.
- `A`: Match the ACK flag.
- `F`: Match the FIN flag.

- `R`: Match the RST flag.
- `U`: Match the URG flag.
- `P`: Match the PSH flag.
- `1`: Match Reserved bit 1.
- `2`: Match Reserved bit 2.
- `0`: Match No TCP flags set.
- `!`: Match if the specified bits are not set.
- `*`: Match if any of the specified bits are set.
- `+`: Match on the specified bits, plus any others.

The first part if the value (`<SAFRUP120>`) defines the bits that must be present for a successful match.

Example:

`--tcp_flags AP` only matches the case where both `A` and `P` bits are set.

The second part (`[,<SAFRUP120>]`) is optional, and defines the additional bits that can be present for a match.

For example `tcp_flags S,12` matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2. The modifiers !, * and + cannot be used in the second part.

window_size

Syntax: `--window_size [!]<window_int>;`

Description:

Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by `0x`. To have the FortiGate search for the absence of the specified window size, add an exclamation mark (`!`) before the window size.

UDP header keywords

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

ICMP keywords

icmp_code

Syntax: `--icmp_code <code_int>;`

Description:

Specify the ICMP code to match.

icmp_id

Syntax: `--icmp_id <id_int>;`

Description:

Check for the specified ICMP ID value.

icmp_seq

Syntax: `--icmp_seq <seq_int>;`

Description:

Check for the specified ICMP sequence value.

icmp_type

Syntax: `--icmp_type <type_int>;`

Description:

Specify the ICMP type to match.

Other keywords

data_size

Syntax: `--data_size {<size_int> | <<size_int> | ><size_int>;`

Description:

Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.

- `<size_int>` is a particular packet size.
- `<<size_int>` is a packet smaller than the specified size.

- `><size_int>` is a packet larger than the specified size.

Examples:

- `--data_size 300;`
- `--data_size <300;`
- `--data_size >300;`

data_at

Syntax: `--data_at <offset_int>[, relative];`

Description:

Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.

dump-all-html

Syntax: `--dump-all-html`

Description:

Dump all HTML files for benchmarking via iSniff. When there is no file type specified, all HTML files are dumped.

rate

Syntax: `--rate <matches_int>,<time_int>;`

Description:

Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.

- `<matches_int>` is the number of times a signature must be detected.
- `<time_int>` is the length of time in which the signature must be detected, in seconds.

  For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If `--rate 100,10;` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. Use this command with `--track` to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.

rpc_num

Syntax: `--rpc_num <app_int>[, <ver_int> | *][, <proc_int> | *>];`

Description:

Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wild card can be used for version and procedure numbers.

same_ip

Syntax: `--same_ip;`

Description:

Check that the source and the destination have the same IP addresses.

track

Syntax: `--track {SRC_IP |DST_IP |DHCP_CLIENT |DNS_DOMAIN}[,block_int];`

Description:

When used with `--rate`, this keyword narrows the custom signature rate totals to individual addresses.

- `SRC_IP`: tracks the packet's source IP.
- `DST_IP`: tracks the packet's destination IP.
- `DHCP_CLIENT`: tracks the DHCP client's MAC address.
- `DNS_DOMAIN`: counts the number of any specific domain name.
- `block_int` has the FortiGate unit block connections for the specified number of seconds, from the client or to the server, depending on which is specified.

  For example, if `--rate 100,10` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiGate unit maintains a single total, regardless of source and destination address.

  If the same custom signature also includes `--track` client; matches are totaled separately for each source address. A log entry is added when the signature is detected 100 times in 10 seconds within traffic from the same source address.

  The `--track` keyword can also be used without `--rate`. If an integer is specified, the client or server will be blocked for the specified number of seconds every time the signature is detected.

Creating a custom signature to block access to example.com

In this first example, you will create a custom signature to block access to the example.com URL.

This example describes the use of the custom signature syntax to block access to a URL. To create the custom signature entry in the FortiGate's GUI, see Custom Application & IPS Signatures.

1. Enter the custom signature basic format.

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords.Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "Block.example.com"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3. Add a signature pattern

Use the `--pattern` keyword to specify what the FortiGate unit will search for:

```
F-SBID( --name "Block.example.com"; --pattern "example.com"; )
```

The signature will now detect the example.com URL appearing in network traffic. The custom signature should only detect the URL in HTTP traffic, however. Any other traffic with the URL should be allowed to pass. For example, an email message to or from example.com should not be stopped.

4. Specify the service

   Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; )
   ```

   The FortiGate unit will limit its search for the pattern to the HTTP protocol. Even though the HTTP protocol uses only TCP traffic, the FortiGate will search for HTTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --
       protocol tcp; )
   ```

   The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network traffic.

6. Ignore case sensitivity

   By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

   Use the `--no_case` keyword to make the pattern matching case insensitive.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --
       protocol tcp; --no_case; )
   ```

   Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7. Limit pattern scans to only traffic sent from the client

   The `--flow` command can be used to further limit the network traffic being scanned to only that send by the client or by the server.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --
       protocol tcp; --no_case; --flow from_client; )
   ```

   Web servers do not contact clients until clients first open a communication session. Therefore, using the `--flow from_client` command will force the FortiGate to ignore all traffic from the server. Since the majority of HTTP traffic flows from the server to the client, this will save considerable system resources and still maintain protection.

8. Specify the context

   When the client browser tries to contact example.com, a DNS is first consulted to get the example.com server IP address. The IP address is then specified in the URL field of the HTTP communication. The domain name will still appear in the host field, so this custom signature will not function without the `--context host` keyword/value pair.

   ```
   F-SBID( --name "Block.example.com"; --pattern "example.com"; --service HTTP; --no_
       case; --flow from_client; --context host; )
   ```

Creating a custom signature to block the SMTP “vrfy” command

The SMTP “vrfy” command can be used to verify the existence of a single email address or to list all of the valid email accounts on an email server. A spammer could potentially use this command to obtain a list of all valid email users and direct spam to their inboxes.

In this example, you will create a custom signature to block the use of the vrfy command. Since the custom signature blocks the vrfy command from coming through the FortiGate unit, the administrator can still use the command on the internal network.

This example describes the use of the custom signature syntax to block the vrfy command. To create the custom signature entry in the FortiGate's GUI, see Custom Application & IPS Signatures.

1. Enter the custom signature basic format

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before you add any other keywords.

   Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic. You must specify a pattern that the FortiGate unit will search for.

3. Add a signature pattern

   Use the `--pattern` keyword to specify what the FortiGate unit will search for:

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; )
   ```

   The signature will now detect the vrfy command appearing in network traffic. The custom signature should only detect the command in SMTP traffic, however. Any other traffic with the pattern should be allowed to pass. For example, an email message discussing the vrfy command should not be stopped.

4. Specify the service.

   Use the `--service` keyword to limit the effect of the custom signature to only the HTTP protocol.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; )
   ```

   The FortiGate unit will limit its search for the pattern to the SMTP protocol.

   Even though the SMTP protocol uses only TCP traffic, the FortiGate will search for SMTP protocol communication in TCP, UDP, and ICMP traffic. This is a waste of system resources that you can avoid by limiting the search further, as shown below.

5. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic.

This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

```
F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --
    protocol tcp; )
```

The FortiGate unit will limit its search for the pattern to TCP traffic and ignore the pattern in UDP and ICMP network traffic.

6. Ignore case sensitivity.

   By default, patterns are case sensitive. If a user directed his or her browser to Example.com, the custom signature would not recognize the URL as a match.

   Use the `--no_case` keyword to make the pattern matching case insensitive.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --no_case; )
   ```

   Unlike all of the other keywords in this example, the `--no_case` keyword has no value. Only the keyword is required.

7. Specify the context.

   The `SMTP vrfy` command will appear in the SMTP header. The `--context host` keyword/value pair allows you to limit the pattern search to only the header.

   ```
   F-SBID( --name "Block.SMTP.VRFY.CMD"; --pattern "vrfy"; --service SMTP; --no_case; -
       -context header; )
   ```

Creating a custom signature to block files according to the file's hash value

In this example, you will create a custom signature that allows you to specify a hash value (or checksum) of a file that you want to block. To block multiple files you can create a custom signature for each file with that file's hash value in it and then add all of the custom signatures to an IPS sensor and set the action to block for each one. When IPS encounters a file with a matching hash value the file is blocked.

This example uses a CRC32 checksum of the file as the hash value of the file to be blocked. You can use any utility that supports CRC32 checksums to generate the hash value.

1. Enter the custom signature basic format.

   All custom signatures have a header and at least one keyword/value pair. The header is always the same:

   ```
   F-SBID( )
   ```

   The keyword/value pairs appear within the parentheses and each pair is followed by a semicolon.

2. Choose a name for the custom signature

   Every custom signature requires a name, so it is a good practice to assign a name before adding any other keywords. Use the `--name` keyword to assign the custom signature a name. The name value follows the keyword after a space. Enclose the name value in double-quotes:

   ```
   F-SBID( --name "File.Hash.Example"; )
   ```

   The signature, as it appears here, will not do anything if you try to use it. It has a name, but does not look for any patterns in network traffic.

3. Specify the traffic type.

   Use the `--protocol tcp keyword` to limit the effect of the custom signature to only TCP traffic. This will save system resources by not unnecessarily scanning UDP and ICMP traffic.

   ```
   F-SBID( --name "File.Hash.Example"; --protocol tcp; )
   ```

   The FortiGate unit will limit its search for the pattern to TCP traffic and ignore UDP and ICMP network

traffic.

4. Add the CRC32 hash value.

   Use the `--crc32` keyword. This indicates that the value that follows is a hexadecimal number that represents the CRC32 checksum of the file. The `--crc32` keyword also requires that you include the file length. The syntax is `--crc32 <checksum>,<file-length>;`. The following example shows the syntax for a file with checksum 51480492 and file length 822.

   ```
   F-SBID( --name "File.Hash.Example"; --protocol tcp; --crc32 51480492,822; )
   ```

Other security profiles considerations

The following topics are included in this section:

Global security profiles across Virtual domains (VDOMs)

Previously, if you enabled virtual domains (VDOMs) on your FortiGate unit, any Security Profiles configuration was limited to the VDOM in which you configured it.

Now Security Profiles can be configured globally across multiple VDOMs. In many VDOM environments, some or all profiles may be commonly-shared, for example an MSSP with "parental controls" configured will most likely have the same Web Filtering and Application Control profiles per VDOM.

Global profiles are configured under **Global > Security Profiles** in the GUI or under the following `config global` commands in the CLI:

- `antivirus profile`
- `application list`
- `dlp sensor`
- `ips sensor`
- `webfilter profile`

The name for any global profile must start with "g-" for identification. Global profiles are available as read-only for VDOM-level administrators and can only be edited or deleted from within the global settings.

Each security feature has at least one default global profile, available for all VDOMs.

Both Global security profile configuration and the various databases used by Security Profiles features are shared. The FortiGuard antivirus and IPS databases and updates to the databases are shared. The FortiGuard web filter and spam filter features access the FortiGuard distribution network and read the same information when checking email for spam and web site categories and classification.

Conserve mode

FortiGate units perform all Security Profiles processing in physical RAM. Since each model has a limited amount of memory, conserve mode is activated when the remaining free memory is nearly exhausted or the AV proxy has reached the maximum number of sessions it can service. While conserve mode is active, the AV proxy does not accept new sessions.

A warning will appear in the top bar of the FortiGate, regardless of which page in the FortiGate GUI you are on.

The AV proxy

Most content inspection the FortiGate unit performs requires that the files, email messages, URLs, and web pages be buffered and examined as a whole. The AV proxy performs this function, and because it may be buffering many files at the same time, it uses a significant amount of memory. Conserve mode is designed to prevent all the component features of the FortiGate unit from trying to use more memory than it has. Because the AV proxy uses so much memory, conserve mode effectively disables it in most circumstances. As a result, the content inspection features that use the AV proxy are also disabled in conserve mode.

All of the Security Profiles features use the AV proxy with the exception of IPS, application control, DoS as well as flow-based antivirus, DLP, and web filter scanning. These features continue to operate normally when the FortiGate unit enters conserve mode.

Entering and exiting conserve mode

A FortiGate unit will enter conserve mode because it is nearly out of physical memory, or because the AV proxy has reached the maximum number of sessions it can service. The memory threshold that triggers conserve mode varies by model, but it is about 20% free memory. When memory use rises to the point where less than 20% of the physical memory is free, the FortiGate unit enters conserve mode.

The FortiGate unit will leave conserve mode only when the available physical memory exceeds about 30%. When exiting conserve mode, all new sessions configured to be scanned with features requiring the AV proxy will be scanned as normal, with the exception of a unit configured with the one-shot option.

Conserve mode effects

What happens when the FortiGate unit enters conserve mode depends on how you have `av-failopen` configured. There are four options:

off

The off setting forces the FortiGate unit to stop all traffic that is configured for content inspection by Security Profiles features that use the AV proxy. New sessions are not allowed but current sessions continue to be processed normally unless they request more memory. Sessions requesting more memory are terminated.

For example, if a security policy is configured to use antivirus scanning, the traffic it permits is blocked while in conserve mode. A policy with IPS scanning enabled continues as normal. A policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the AV proxy.

Use the off setting when security is more important than a loss of access while the problem is rectified.

pass

The pass setting allows traffic to bypass the AV proxy and continue to its destination. Since the traffic is bypassing the proxy, no Security Profiles scanning that requires the AV proxy is performed. Security Profiles scanning that does not require the AV proxy continues normally.

Use the pass setting when access is more important than security while the problem is rectified.

Pass is the default setting.

one-shot

The one-shot setting is similar to pass in that traffic is allowed when conserve mode is active. The difference is that a system configured for one-shot will force new sessions to bypass the AV proxy even after it leaves conserve mode. The FortiGate unit resumes use of the AV proxy only when the `av-failopen` setting is changed or the unit is restarted.

idledrop

The idledrop setting will recover memory and session space by terminating all the sessions associated with the host that has the most sessions open. The FortiGate may force this session termination a number of times, until enough memory is available to allow it to leave conserve mode.

The idledrop setting is primarily designed for situations in which malware may continue to open sessions until the AV proxy cannot accept more new sessions, triggering conserve mode. If your FortiGate unit is operating near capacity, this setting could cause the termination of valid sessions. Use this option with caution.

Configuring the av-failopen command

You can configure the av-failopen command using the CLI.

```
config system global
   set av-failopen {off | pass | one-shot | idledrop}
end
```

The default setting is pass.

Using wildcards and Perl regular expressions

Many Security Profiles feature list entries can include wildcards or Perl regular expressions.

For more information about using Perl regular expressions, see http://perldoc.perl.org/perlretut.html.

Regular expression vs. wildcard match pattern

A wildcard character is a special character that represents one or more other characters. The most commonly used wildcard characters are the asterisk (*), which typically represents zero or more characters in a string of characters, and the question mark (?), which typically represents any one character.

In Perl regular expressions, the '.' character refers to any single character. It is similar to the '?' character in wildcard match pattern. As a result:

- example.com not only matches example.com but also examplea.com, exampleb.com, examplec.com, and so on.

To add a question mark (`?`) character to a regular expression from the FortiGate CLI, enter Ctrl+V followed by ?. To add a single backslash character (`\`) to a regular expression from the CLI you must add precede it with another backslash character. For example, `example\\.com`.

To match a special character such as '.' and '*' use the escape character '\'. For example:

- To match example.com, the regular expression should be: example\.com

In Perl regular expressions, '*' means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- exam*.com matches exammmm.com but does not match example.com

To match any character 0 or more times, use '.*' where '.' means any character and the '*' means 0 or more times. For example, the wildcard match pattern exam*.com should be exam.*\.com.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression "test" not only matches the word "test" but also any word that contains "test" such as "atest", "mytest", "testimony", "atestb". The notation "\b" specifies the word boundary. To match exactly the word "test", the expression should be \btest\b.

Case sensitivity

Regular expression pattern matching is case sensitive in the web and Email Filter filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of "bad language", regardless of case.

Perl regular expression formats

The following table lists and describes some example Perl regular expressions.

Perl regular expression formats

Expression	Matches
abc	"abc" (the exact character sequence, but anywhere in the string)
^abc	"abc" at the beginning of the string
abc$	"abc" at the end of the string
a|b	Either "a" or "b"
^abc|abc$	The string "abc" at the beginning or at the end of the string
ab{2,4}c	"a" followed by two, three or four "b"s followed by a "c"
ab{2,}c	"a" followed by at least two "b"s followed by a "c"
ab*c	"a" followed by any number (zero or more) of "b"s followed by a "c"
ab+c	"a" followed by one or more b's followed by a c
ab?c	"a" followed by an optional "b" followed by a" c"; that is, either "abc" or "ac"
a.c	"a" followed by any single character (not newline) followed by a" c "

Expression	Matches
a\.c	“a.c” exactly
[abc]	Any one of “a”, “b” and “c”
[Aa]bc	Either of “Abc” and “abc”
[abc]+	Any (nonempty) string of “a”s, “b”s and “c”s (such as “a”, “abba”, ”acbabcacaa”)
[^abc]+	Any (nonempty) string which does not contain any of “a”, “b”, and “c” (such as “defg”)
\d\d	Any two decimal digits, such as 42; same as \d{2}
/i	Makes the pattern case insensitive. For example, `/bad language/i` blocks any instance of `bad language` regardless of case.
\w+	A “word”: A nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	The strings “100” and “mk” optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	“abc” when followed by a word boundary (for example, in “abc!” but not in “abcd”)
perl\B	“perl” when not followed by a word boundary (for example, in “perlert” but not in “perl stuff”)
\x	Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into (slightly) more readable parts.
/x	Used to add regular expressions within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/'. The pattern between ‘/’ will be taken as a regular expressions, and anything after the second ‘/’ will be parsed as a list of regular expression options ('i', 'x', etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Examples of regular expressions

Block any word in a phrase

```
/block|any|word/
```

Block purposely misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*o.*$/i
/cr[eéèêë][\+\-\*=<>\.\,;!\?%&§@\^°\$£€\{\}()\[\]\|\\_01]dit/i
```

Block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

```
/try it for free/i
/student loans/i
/you're already approved/i
/special[\+\-\*=<>\.\,;!\?%&~#§@\^°\$£€\{\}()\[\]\|\\_1]offer/i
```

Control how sessions are distributed to Fortinet processes

Previously, the explicit web proxy balanced the client to a specific WAD daemon based only on the source IP. There are cases where customers use another explicit proxy in front of the FortiGate. With such a design, the FortiGate can see the traffic originating from only one IP address (or a small set of IP addresses) and utilize only one (or a small number) of WAD processes.

This new feature modifies the wad-worker balancing algorithm to also use the source port in addition to source IP when distributing the client to a specific WAD daemon. With this in place, even the connections from one IP address will be balanced over all the WAD processes. This also avoids the degraded performance results for the cases where customers are testing the FortiGate as the explicit webproxy to replace Bluecoats, but don't want to remove Bluecoats from the network for the PoC.

Syntax

```
config system global
   set wad-source-affinity {enable | disable}
end
```

This feature is enabled by default. Disabling this option results in some features to be unsupported. IP-based user authentication, disclaimer messages, security profile override, authentication cookies, MAPI scanning, and some video caches such as Youtube are not supported.

CPU allocation and tuning commands to survive reboot

CPU affinity, whereby a process will execute on a specific CPU, can be changed so it survives a reboot.

CLI syntax:

```
config system global
   set av-affinity
   set ips-affinity
   set miglog-affinity
end
```

av-affinity: Affinity setting for AV scanning (64-bit hexadecimal value in the format of xxxxxxxx_xxxxxxxx).

ips-affinity: Affinity setting for IPS (64-bit hexadecimal value in the format of xxxxxxxx_xxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons). This option is only available if the FortiGate includes NP6 processors and support NTurbo.

miglog-affinity: Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxx_xxxxxxxx).

Excluding industrial IP signatures

To reduce performance impacts caused by industrial IP signatures, the admin can choose to exclude the industrial signatures when they are loaded by IPS; the industrial signatures then become inactive as a result. The following CLI command has been restored for this purpose.

Syntax

```
config ips global
   set exclude-signatures {none | industrial}
end
```